Serving the police community since 1938

GAZETTE

WORST-CASE SCENARIO

TAKING PREPAREDNESS TO THE NEXT LEVEL

LEARNING FROM SARS
Lessons from the Toronto police

ADAPTING TO TERROR
Israeli civilians prove resilient

WILDLIFE COLLISIONS
Changing animal behaviour

Royal Canadian Gendarmerie royale
Mounted Police du Canada

Canadä

Readying for the next big one

About 10 years ago, a tornado ripped through my hometown. Several houses were completely destroyed, throwing numerous residents into homelessness. Police, firefighters and emergency medical workers arrived quickly on the scene, tending to the injured and blocking off the affected area for safety and security reasons. The municipal emergency plan also kicked into gear, offering shelter and support.

It was my first glimpse of a large-scale emergency response. It reinforced that, despite the city's detailed disaster plan, there are always surprises.

In this issue on emergency preparedness and response, we look at how police agencies are readying themselves for the next event — be it a natural disaster, a public health crisis or terrorism — and trying to minimize those surprises.

We begin with how the RCMP is preparing for a pandemic, an event that public health experts say is inevitable, even overdue. The RCMP's Operational Readiness and Response Coordination Centre addresses not only operational preparedness in emergency situations, but personal readiness for every employee. The key, say emergency management experts, is getting people engaged before the crisis hits.

While there hasn't been an influenza pandemic since the 1960s, the 2003 SARS outbreak in Toronto served as a wake-up call for many about the potential spread of an infectious disease. S/Supt Peter Sloly and S/Sgt Scott Roberts of the Toronto Police Service share that service's experiences in responding to the crisis from day one of the outbreak through to the city's recovery efforts.

Technology plays a role in preparing for and responding to a disaster. Luc Filion of the RCMP's Mobile Communication Services looks at the challenges of communicating in tense situations when the radio systems of numerous emergency responders are not interoperable and what is being done to remedy that problem. Geoff Coulson, a warning preparedness meteorologist with Environment Canada, describes how technology together with volunteer networks, including police, can improve the accuracy of severe weather predictions.

We invited Alain Normand, an emergency manager with the City of Brampton, to provide some useful tips to police on preparing for the various roles they may play in a disaster. Where do you begin? He says start with the municipal emergency plan nearest you.

When the emergency has happened, one challenge is getting accurate information out to the public. Joseph Scanlon is an emergency communications expert at Carleton University and he shares advice about what to say and do — before, during and after a crisis.

We also look at what emergencies are being dealt with outside of Canada. Jessica Davison of the Victoria Police in Australia describes one of the worst bushfire seasons on record, and how all first responders made communication and co-ordination a priority when warning and evacuating communities at risk.

Professor Alan Kirschenbaum of the Technion–Israel Institute of Technology explores the topic of community resilience in Israel where many residents live with the daily threat of terrorism. Contrary to what many people assume, his research shows that humans display a remarkable ability to adapt — even thrive — during uncertain times.

Finally, the U.S. National Institute of Justice conducted research on the significant impact of an agro-terrorism attack on that country. It suggests that law enforcement agencies will be pushed to the limits and must begin now to develop response plans, alongside agricultural experts, to be ready.

Reducing that element of surprise is what it's all about. We hope this issue gets our readers thinking about their own preparedness.

Katherine Aldred

More to explore on emergency preparedness and response from the Canadian Police College Library

www.cpc.gc.ca/library_e.htm

Books

Disaster Resilience: An Integrated Approach / Paton, Douglas. Springfield, IL, USA: Charles C. Thomas. HV 553 P27 2006

Emergency Preparedness for Transit Terrorism / Boyd, Annabelle. Washington, D.C. USA: Transportation Research Board. HE 4456 B69 1997.

Articles

L'impact d'un désastre sur les comportements d'entraide et les niveaux de criminalité / Lemieux, Frédéric. Revue internationale de criminologie et de police technique et scientifique Vol. 59, No. 1, 2006, pp. 3-20.

Pas de vacances pour les risques ... / Leboeuf, Alain. Sécurité Vol. 7, No. 4, 2003, pp.30.

SARS Outbreak 2003: The Response of the Toronto Police Service / Fantino, Julain. Police Chief Vol. 72, No. 4, 2005, pp. 22, 24-28.

Shared Plans Protect and Save Lives / Galvin, Bob. Law Enforcement Technology Vol. 32, No. 7, 2005. pp. 132, 134-137.

Using the Community Policing Model for Approaching Terrorist Threats and Domestic Preparedness / Morreale, Stephen A. Law Enforcement Executive Forum Vol. 4, No. 7, 2004, pp. 121-134.

Readying for the next big one

About 10 years ago, a tornado ripped through my hometown. Several houses were completely destroyed, throwing numerous residents into homelessness. Police, firefighters and emergency medical workers arrived quickly on the scene, tending to the injured and blocking off the affected area for safety and security reasons. The municipal emergency plan also kicked into gear, offering shelter and support.

It was my first glimpse of a large-scale emergency response. It reinforced that, despite the city's detailed disaster plan, there are always surprises.

In this issue on emergency preparedness and response, we look at how police agencies are readying themselves for the next event — be it a natural disaster, a public health crisis or terrorism — and trying to minimize those surprises.

We begin with how the RCMP is preparing for a pandemic, an event that public health experts say is inevitable, even overdue. The RCMP's Operational Readiness and Response Coordination Centre addresses not only operational preparedness in emergency situations, but personal readiness for every employee. The key, say emergency management experts, is getting people engaged before the crisis hits.

While there hasn't been an influenza pandemic since the 1960s, the 2003 SARS outbreak in Toronto served as a wake-up call for many about the potential spread of an infectious disease. S/Supt Peter Sloly and S/Sgt Scott Roberts of the Toronto Police Service share that service's experiences in responding to the crisis from day one of the outbreak through to the city's recovery efforts.

Technology plays a role in preparing for and responding to a disaster. Luc Filion of the RCMP's Mobile Communication Services looks at the challenges of communicating in tense situations when the radio systems of numerous emergency responders are not interoperable and what is being done to remedy that problem. Geoff Coulson, a warning preparedness meteorologist with Environment Canada, describes how technology together with volunteer networks, including police, can improve the accuracy of severe weather predictions.

We invited Alain Normand, an emergency manager with the City of Brampton, to provide some useful tips to police on preparing for the various roles they may play in a disaster. Where do you begin? He says start with the municipal emergency plan nearest you.

When the emergency has happened, one challenge is getting accurate information out to the public. Joseph Scanlon is an emergency communications expert at Carleton University and he shares advice about what to say and do — before, during and after a crisis.

We also look at what emergencies are being dealt with outside of Canada. Jessica Davison of the Victoria Police in Australia describes one of the worst bushfire seasons on record, and how all first responders made communication and co-ordination a priority when warning and evacuating communities at risk.

Professor Alan Kirschenbaum of the Technion–Israel Institute of Technology explores the topic of community resilience in Israel where many residents live with the daily threat of terrorism. Contrary to what many people assume, his research shows that humans display a remarkable ability to adapt — even thrive — during uncertain times.

Finally, the U.S. National Institute of Justice conducted research on the significant impact of an agro-terrorism attack on that country. It suggests that law enforcement agencies will be pushed to the limits and must begin now to develop response plans, alongside agricultural experts, to be ready.

Reducing that element of surprise is what it's all about. We hope this issue gets our readers thinking about their own preparedness.

Katherine Aldred

More to explore on emergency preparedness and response from the Canadian Police College Library

www.cpc.gc.ca/library_e.htm

Books

Natural Hazards: An Integrated Approach / Paton, Douglas. Springfield, IL, USA: Charles C. Thomas, HV 553 P37 2006.

Emergency Preparedness for People with Disabilities / Boyd, Annabelle. Washington, D.C., USA: Transportation Research Board, HE 4456 B69 1997.

Articles

Impact d'un désastre sur les comportements d'entraide et les niveaux de criminalité / Lemieux, Frédéric. Revue internationale de criminologie et de police technique et scientifique Vol. 59, No. 1, 2006, pp. 3-20.

Pas de vacances pour les risques... / Leboeuf, Alain. Sécurité Vol. 7, No. 4, 2003, pp. 30.

SARS Outbreak 2003: The Response of the Toronto Police Service / Fantino, Julian. Police Chief Vol. 72, No. 4, 2005, pp. 22, 24-28.

Shared Plans Protect and Save Lives / Galvin, Bob. Law Enforcement Technology Vol. 32, No. 7, 2005, pp. 132, 134-137.

Using the Community Policing Model for Approaching Terrorist Threats and Domestic Preparedness / Nicastro, Stephen A. Law Enforcement Executive Forum Vol. 4, No. 7, 2004, pp. 121-134.

GAZETTE

RCMP E Division

Police and firefighters respond to a landslide in Terrace, B.C. last June, which blocked the town's only road access and resulted in two deaths.
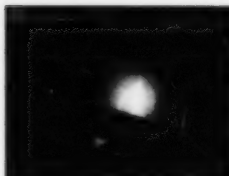
Cover

Departments

ON THE COVER

Preparing for emergencies is not new, but developing rigorous readiness plans for today's increasingly complex emergencies — from severe weather to terrorism to pandemic influenza — is the key to effective response and recovery.

TEAMS TACKLE COUNTERFEIT CURRENCY

Officially launched in May, the RCMP's Integrated Counterfeit Enforcement Teams (ICETs) have already made great strides in the fight against counterfeit currency in Canada.

Significant counterfeit enforcement successes have been seen across the country since the teams were originally established in 2006. Seizures of counterfeit bank notes and the equipment used to produce them have taken millions of fake dollars out of circulation.

Most recently Operation Ophir, an 18-month investigation in Toronto, led to the dismantling of the largest known counterfeiting plant in Canadian history. The plant was using complex commercial

This gym bag filled with counterfeit $20 bills is a small example of the counterfeit currency that ICETs are helping to take out of circulation.

grade printing equipment, capable of manufacturing large quantities of Canadian and U.S. counterfeit currency, and counterfeit payment and identification cards.

"Over $6 million in counterfeit bank notes, found in every province in Canada, has been attributed to this plant," says RCMP S/Sgt Ken MacDonald, ICET team leader in Toronto West Detachment. "This has been a huge success, especially within the first year of the launch of the ICETs."

Formed as part of the National Counterfeit Enforcement Strategy (NCES), the ICETs are strategically located in Toronto, Montreal and Vancouver, the three areas in Canada where counterfeit currency activity is highest. There are also regional counterfeit co-ordinators located in Calgary and Halifax.

The teams are mandated to investigate cases where organized crime groups are involved in the production or high-volume distribution of counterfeit currency. The teams liaise with local law enforcement agencies to share information and work with Bank of Canada regional representatives to develop and deliver public education and awareness programs.

"This puts much more emphasis on proactive enforcement by all RCMP entities," says Insp Barry Baxter of the Commercial Crime Branch.

And the approach is working. In 2004, Canada's worst year for counterfeit bank notes according to Insp Baxter, more than

This printing equipment and counterfeit money was seized during Operation Ophir, which led to the dismantling of the largest known counterfeiting plant in Canadian history.

648,000 counterfeit bills were found in circulation or seized, representing a value of just over $16 million.

In contrast, in 2006, the first year ICETs were in place, about 322,000 bank notes were found or seized, representing a value of about $9 million. Insp Baxter attributes the dramatic decrease to the work of the ICETs, the state-of-the-art security features on the new 2004 series of Canadian banknotes and increased public awareness.

"This shows what proactive enforcement by dedicated teams can do," says Baxter. "We're seeing the results."

—Susan Demaray

A BLAST OF A WORKSHOP

When the RCMP's Post-Blast National Response team gathered for a workshop just north of Quebec City, from September 17-21, 2007, they were joined by colleagues from around Canada and the world.

Members from police and army forces from as far away as Singapore, Australia, and Europe were on hand to observe and share their expertise with RCMP Post-Blast team members, forensic specialists and other regional and provincial police members.

"It's a chance to exchange information and to have these people here as expert consultants," says S/Cst Jean-Yves Vermette, the organizer of the post-blast workshop. "Incidents here could be happening over there as well. We'll be better able to assist each other because we'll have the expertise these workshops provide."

Having the opportunity to experience the scene of an explosion where no one is hurt gives investigators a chance to learn and build their knowledge of explosives and the damage they cause.

"In real life you don't get the opportunity to visit sites of explosions in situations where you can learn and if mistakes happen

it's not important," says Stefan Klein, detective inspector for the Federal Criminal Police Office and the National Bomb Data Centre in Wiesbaden, Germany.

"If you see a site of an explosion for the first time, it is hard to imagine what power and velocity is going on. But if you can compare it to something — it looks like this amount of explosive, for example — you can get an idea of what was going on."

Antonio Acevedo, a subinspector and bomb technician with the Madrid CBRNE Central Unit of the Spanish Police Force and a member of the Bomb Data Centre of Spain was one of the few participants at the workshop with first-hand knowledge

Estimates on the amount of money laundered per year worldwide range in the hundreds of billions of dollars (U.S.). This figure shows not only the global scale of money laundering, but also indicates that the methods available for laundering money are legion.

Many books on the subject present these issues of scale and variation as being virtually insurmountable — pointing out the discrepancies in national laws and gaps in monitoring that allow money laundering to proliferate. The Commonwealth Secretariat's book on the subject takes an entirely different stance. Rather than focusing on the flaws in current money laundering countermeasures, Combating Money Laundering and Terrorist Financing examines how governments and companies severely limit criminal and terrorist access to legitimate financial systems.

To this end, this book examines the three levels of money laundering countermeasures — global, national and professional — from every possible angle, creating a holistic perspective on problems and solutions. This allows readers at all levels, from policy-makers to professionals in various businesses, to clearly see their role in detecting and preventing money laundering.

On the global level, the book examines how collaboration between regional financial intelligence units can be better used to create a global framework. This book also discusses not only why enforcement agencies from different countries must co-operate, but provides strategies for information sharing and mutual reinforcement of international conventions.

On a professional level, this book provides practical frameworks for customer due diligence, suspicious transaction reporting and legal compliance. It also addresses how businesses such as real estate brokers and precious metals dealers are targeted by criminals and terrorists and what countermeasures can be used to prevent money laundering. This is a highly valuable addition as most books on money laundering limit coverage to banks and wire transferors.

In addition, this second edition includes expanded coverage of terrorist financing methods and new international standards for money laundering countermeasures.

Combating Money Laundering and Terrorist Financing is a relatively short book that paints a broad picture of money laundering rather than delving into the finer points. This allows the reader to obtain a comprehensive overview of money laundering and terrorist financing, including the problems and solutions at all levels of involvement. For many professionals, this coverage is sufficient for formulating customer due diligence policies and procedures for suspicious transaction reporting.

In all, this book should be required reading for anyone with a role in creating or enforcing money laundering countermeasures, or for anyone who is tired of books that simply hype the money laundering problem without offering any real solutions.

Dan Bergevin is a compliance consultant and journalist who specializes in international financial affairs. He currently lives and works in Salt Lake City, Utah.

of how to work a scene of a major explosion. He was one of the police officers who worked on site after the Madrid train bombings in 2004. He says that when faced with the unthinkable, you simply do your job.

"In the hardest moments, everyone has to be ready," he says. "We are the only people who couldn't cry. We must stay okay."

Acevedo says he came to the workshop to learn a different point of view. For example, while the Spanish police work in a grid system when collecting evidence, it is a different system than the grids RCMP forensic teams set up. "There are different ways to do the same work that I do," he says. "Even if they are just little detail points that differ, it's interesting to me, and helps me improve."

Both Klein and Acevedo agree that while no one wants to think an event like a terrorist attack or other explosion could happen in their country, it's important to remain up-to-date on the latest explosive technology and forensic techniques.

"The best way to protect your country is to avoid having things happen — but you have to be prepared," Klein says. "You can't wait for it, but you can be prepared for it."

—*Susan Demaray*

Officers from Germany (left) and Spain (right) walk with an RCMP member during a post-blast workshop held this fall in Quebec City. The workshop allowed participants to share knowledge and tips with one another while working on a simulated explosion investigation.

Combing hair for clues
Hair sampling reveals travel patterns

Give Della Wilkinson a few strands of your hair, and she can tell with surprising accuracy where you lived or travelled in the time it took that hair to grow. Wilkinson, a scientist with National Services and Research at the RCMP, is involved in an international project that uses isotopes in hair as a geolocatory tool — a technique that is already proving useful in forensic investigations. The Gazette's *Caroline Ross spoke with Wilkinson about her research.*

What are isotopes?
Isotopes are chemical elements that have similar chemical properties but different masses. Stable isotopes stay around for a long time and don't degrade or decay. Hydrogen has stable isotopes, as do several other elements such as carbon, nitrogen and oxygen. Fortunately for forensic scientists, these stable isotopes are found in the food that we eat and the water that we drink.

What is the link between isotopes and hair?
We know that different cities and countries may have different isotope ratios in their water supplies, due to precipitation patterns and environmental conditions. As hair grows, these isotopes should be incorporated into the core structure of the hair in a chronological order. By sampling particular portions of your hair and measuring the isotope ratios, we should be able to see travel patterns. For example, if a Canadian travels to Africa or Australia, you should see significant changes in their isotope ratios.

How did the RCMP become involved with isotopes and hair sampling?
I represent the RCMP on the Investigative Support and Forensics subgroup of the Technical Support Working Group on counterterrorism. During one meeting, I was approached by a colleague from the U.S. who described a project that they had called FIRMS, which stands for Forensic Stable Isotope Ratio Mass Spectrometry. They were collecting hair, water and protein samples from around the globe, trying to build a global map of oxygen, hydrogen, nitrogen and carbon isotope ratios. In return for our participation in helping to collect samples, they were willing to share the database with us.

How would access to that information benefit the RCMP?
From a criminal perspective, there is already an interest in unidentified human remains where there is no missing persons report that matches the individual. For police, it would be incredibly valuable if you could determine if that person was local or not. Hypothetically, you could use the FIRMS database to point you to a community, region or country outside Canada where that person may have originated.

Can you give me an example of how isotopes helped solve a case?
In the U.K., there was an unidentified female found in Manchester, in the north of England. There had been no missing persons reports in any of the nearby constabularies, so they had absolutely no leads. But they sent the hair for analysis and were able to determine that the person had never lived in Manchester. The hair isotopes were consistent with a person living in one place for a long period of time, and that place was London. The investigation shifted from the North to the South, and, based on other information that they got from isotopes within the diet, they were able to determine that the person had illegally immigrated to London and then been murdered. Obviously, there was a lot more information that came in, but that little lead at the beginning was very important.

What is the next step in your project?
Right now we are populating the database in the States. Hopefully, the next round will build on that within Canada. I look at the U.S. study more as a seed project. You learn a lot by doing these projects. First of all, you answer the question, "Is it worth continuing? Is there really some value here?" and, yes, that seems to have definitely been demonstrated. ■

Della Wilkinson, RCMP research scientist, examines a vial used to collect hair and water samples that can reveal a person's travel patterns.

Caroline Ross

PREPARING FOR A PANDEMIC
NATIONAL PLAN STARTS WITH INDIVIDUAL READINESS

By Katherine Aldred

The estimates speak for themselves. According to the Public Health Agency of Canada (PHAC), over the course of an influenza pandemic, up to 70 per cent of the population will become infected and between 15 and 35 per cent will become clinically ill and miss work. If antivirals are not available, 1 per cent of the ill will be hospitalized and 0.4 per cent will die.

Unlike most other types of disasters, an influenza pandemic will not be limited to one or two locations. When a major new influenza virus occurs, it will spread easily from human to human resulting in

enormous numbers of deaths and illness.

"We don't know when a pandemic will occur, what the cause will be, how severe it will be or who will be hardest hit," says Dr. Arlene King, director general for Pandemic Preparedness at PHAC. "We do know one thing: when any emergency hits, it's too late to be doing the planning. The structures, processes and tools have to be in place."

Police agencies involved in responding to a pandemic must be prepared not only to deal with the complex requirements of a public health emergency but to carry on their normal day-to-day operations with a greatly diminished workforce. The challenge is getting ready.

Operational readiness

The RCMP's Operational Readiness and Response Co-ordination Centre (ORRCC)

in Ottawa was created in 2006 to help provide the necessary planning, resources and support across the country to respond to any emergency, including a public health crisis.

ORRCC's focus is on providing national leadership, guidance, support and a single point of contact for all key elements of emergency management. While its central secretariat is located in Ottawa, the centre exists to support police operations across Canada when needed.

"An emergency is a local response issue," says A/Commr John Neily, head of the ORRCC. "My role here is to co-ordinate the work in the local area when they need the help and look at what's happening across the country. Most (provinces) are able to hold their own but on occasion they'll need some special

support. We're going to have the protocols in place to be able to do that for them seamlessly."

One important initiative that falls under ORRCC is pandemic preparedness. Although the Public Health Agency of Canada will take a lead role in protecting Canadians during a pandemic by maintaining the Canadian Pandemic Influenza Plan, ensuring a contract for the production of a pandemic vaccine, creating a national antiviral stockpile, monitoring the global situation and increasing public awareness among other things, it will do so with the support of provincial and territorial governments and other federal government

departments, including the RCMP.

According to Neily, the RCMP could be called in to provide a number of different functions during a pandemic such as enforcing public health orders like quarantines and travel restrictions, limiting access to areas deemed out of bounds, transporting and protecting medical equipment or medications, protecting certain types of facilities and, in a worst-case scenario, controlling crowds.

And like any operational response, police must be prepared for the conditions — in this case, a contagious disease.

Occupational health

The RCMP's Occupational Health Section is involved in ensuring that standards are in place to protect employees who respond during a pandemic.

Dr. Jean-Pierre Legault is the director of Occupational Health at the RCMP and has been central in developing health guidelines for pandemic flu preparedness and response. The guidelines outline everything from explaining what pandemic influenza is, identifying the operational risks for front-line responders, listing the best measures for preventing and managing infection, and describing the types of personal protective equipment recommended and how each should be used.

"From a health point of view, our preparedness plan outmatches anything out there," says Legault. "One of the greatest challenges will be trying to assist with public order and containment measures to prevent the spread of the virus while a vaccine is being developed. We may also be enforcing social distancing measures and there are always people who do not want to follow that."

RCMP employees are starting to be trained in these roles. For instance, under the federal *Quarantine Act*, the PHAC provides the necessary training and equipment for RCMP members so they are prepared to help enforce the Act at major airport centres and ports of entry. To date, about 300 members in key locations have received the training.

Personal preparedness

In addition to operational readiness, one of the key messages that emergency planners are sending to employees is to be personally prepared.

Large-scale emergencies pose unique psychological, social and physical challenges even for experienced first responders. Because many employees live in the same communities in which they serve, there is a good chance they will be personally affected when disaster strikes. This could result in not reporting for work or being distracted out of concern for their families or their own personal safety.

For instance, knowing the risks of exposure to a flu pandemic and how to minimize them is one way employees and their families can be prepared. Getting an annual influenza shot is another.

Erickson has already had some experience in raising awareness about employee preparedness. Severe flooding in British Columbia last summer meant that many members had to be prepared to report to work even if their own homes and communities were affected.

Erickson says as part of the preparation, they looked at the possibility of floods taking out roadways and communications

> " If our people are not personally prepared to be at work with the comfort that their loved ones are being taken care of, then we are going to have a challenge.
>
> *A/Commr John Neily* "

"Workforce resilience is the underpinning of everything that we do," says Neily. "If our people are not personally prepared to be at work with the comfort that their loved ones are being taken care of, then we are going to have a challenge."

This human factor in emergency and continuity planing is now a key component of readiness, especially following Hurricane Katrina, where many first responders fell victim to burn-out made worse by uncertainty about their own families' safety. A pandemic could present the same challenges.

"Our employees are no different from the general public," says Insp Dennis Erickson, program manager for the RCMP's Operational Readiness and Response Co-ordination Centre (ORRCC) in British Columbia. "In a pandemic, we are going to be just as affected as everybody else. The biggest issue is going to be our individual preparedness mind set. When we experience a pandemic-like event, it's going to be how we deal with it as individual employees."

systems. Aside from providing employees with alternate work sites, the ORRCC sent out regular communiques to update employees and set up a phone-in line where they could call in to get help. They also encouraged employees to come up with their own emergency plans.

"I often feel that I have a hard time selling the next big earthquake or that a pandemic is coming," says Erickson. "To me, individual preparedness will be the biggest risk if we don't do it right, and the biggest save if we get our people engaged in it."

Dr. King reinforces the point of not becoming complacent, citing what she calls "pandemic fatigue" in planning and preparing for a crisis that seems far off.

"We've been working really hard to prepare for a pandemic and yet we're wondering when this thing is going to happen," says King. "The good news is that we are all working together and this is going to improve our ability to respond to a pandemic or any emerging infectious disease. It's about having the right people in the right place." ∎

How can I protect myself and my family from an influenza pandemic?

- Get your seasonal influenza shot every year — the "flu" shot will not protect you from an influenza pandemic virus, but it will protect you from getting ordinary/seasonal flu, which could weaken your immune system or resistance.

- Wash your hands with soap thoroughly and often — good hand hygiene is the best way to prevent the spread of all viruses.

- Keep an alcohol-based sanitizer (gel or wipes) handy at work, home and in the car (hand sanitizers should contain 60-90 per cent alcohol).

- Cover your mouth and nose with a tissue when you cough or sneeze, dispose of the tissue after use and always wash your hands as a last step.

- If a tissue is not available, cough or sneeze into your sleeve.

- Stay home when you are sick.

- Avoid large crowds of people where viruses can spread easily.

Source: Government of Ontario

Links

Public Safety Canada
www.getprepared.ca

Public Health Agency of Canada
www.influenza.gc.ca

Personal preparedness

In addition to operational readiness, one of the key messages that emergency planners are sending to employees is to be personally prepared.

Large-scale emergencies pose unique psychological, social and physical challenges even for experienced first responders. Because many employees live in the same communities in which they serve, there is a good chance they will be personally affected when disaster strikes. This could result in not reporting for work or being distracted out of concern for their families or their own personal safety.

For instance, knowing the risks of exposure to a flu pandemic and how to minimize them is one way employees and their families can be prepared. Getting an annual influenza shot is another.

Erickson has already had some experience in raising awareness about employee preparedness. Severe flooding in British Columbia last summer meant that many members had to be prepared to report to work even if their own homes and communities were affected.

Erickson says as part of the preparation, they looked at the possibility of floods taking out roadways and communications

> " If our people are not personally prepared to be at work with the comfort that their loved ones are being taken care of, then we are going to have a challenge.
>
> *A/Commr John Neily* "

"Workforce resilience is the underpinning of everything that we do," says Neily. "If our people are not personally prepared to be at work with the comfort that their loved ones are being taken care of, then we are going to have a challenge."

This human factor in emergency and continuity planning is now a key component of readiness, especially following Hurricane Katrina, where many first responders fell victim to burn-out made worse by uncertainty about their own families' safety. A pandemic could present the same challenges.

"Our employees are no different from the general public," says Insp Dennis Erickson, program manager for the RCMP's Operational Readiness and Response Co-ordination Centre (ORRCC) in British Columbia. "In a pandemic, we are going to be just as affected as everybody else. The biggest issue is going to be our individual preparedness mind set. When we experience a pandemic-like event, it's going to be how we deal with it as individual employees."
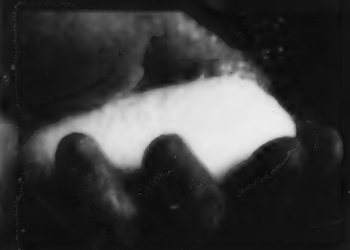
systems. Aside from providing employees with alternate work sites, the ORRCC sent out regular communiques to update employees and set up a phone-in line where they could call in to get help. They also encouraged employees to come up with their own emergency plans.

"I often feel that I have a hard time selling the next big earthquake or that a pandemic is coming," says Erickson. "To me, individual preparedness will be the biggest risk if we don't do it right, and the biggest save if we get our people engaged in it."

Dr. King reinforces the point of not becoming complacent, citing what she calls "pandemic fatigue" in planning and preparing for a crisis that seems far off.

"We've been working really hard to prepare for a pandemic and yet we're wondering when this thing is going to happen," says King. "The good news is that we are all working together and this is going to improve our ability to respond to a pandemic or any emerging infectious disease. It's about having the right people in the right place."

How can I protect myself and my family from an influenza pandemic?

- Get your seasonal influenza shot every year — the "flu" shot will not protect you from an influenza pandemic virus, but it will protect you from getting ordinary/seasonal flu, which could weaken your immune system or resistance.

- Wash your hands with soap thoroughly and often — good hand hygiene is the best way to prevent the spread of all viruses.

- Keep an alcohol-based sanitizer (gel or wipes) handy at work, home and in the car (hand sanitizers should contain 60–90 per cent alcohol).

- Cover your mouth and nose with a tissue when you cough or sneeze, dispose of the tissue after use and always wash your hands as a last step.

- If a tissue is not available, cough or sneeze into your sleeve.

- Stay home when you are sick.

- Avoid large crowds of people where viruses can spread easily.

Source: Government of Ontario

Links
Public Safety Canada
www.getprepared.ca

Public Health Agency of Canada
www.influenza.gc.ca

Opening the floodgates

Information-sharing key to protecting critical infrastructure

By Caroline Ross

Hurricane Katrina damaged utilities, roads, communications and other critical services in New Orleans. Canadian infrastructure stakeholders are joining forces to improve their collective ability to manage similar catastrophes.

FEMA/Andrea Booher

An ice storm cuts power across Eastern Canada. A bomb in a Toronto subway cripples the city's urban transit network.

Critical infrastructure emergencies like these could happen tomorrow. Is Canada's national police force prepared for them?

Canada's critical infrastructure — the physical and information systems that underpin Canadian health, safety, security and economic well-being — presents a particular challenge for emergency planners. Over 85 per cent of Canadian critical infrastructure is privately, provincially or territorially owned, and proprietary interests can limit access to details about infrastructure operations and vulnerabilities. Information-sharing among private and public sector partners is therefore crucial to effective emergency planning and prevention activities.

For the RCMP's emergency management team, information-sharing is the keystone of critical infrastructure emergency preparedness. The team has been consulting with Canada's critical infrastructure operators since 2001 to create a set of emergency operations templates that detail the police response for infrastructure emergencies such as blackouts, floods and terrorist acts.

RCMP emergency operations managers in each province and territory then take the templates to their local partners — energy companies, municipal bodies, local police, etc. — to hammer out the details of a community-specific response.

"We reached out to public and private sector subject matter experts and said, 'Here's what we've got. Now we need your input to do it,'" says Brian Porrior, officer in charge of emergency management at RCMP Headquarters.

The work feeds into public and private sector planning activities and ensures that emergency management plans at all levels are plugged into one another.

Sgt Mike Self, emergency operations manager with the Alberta RCMP, describes how his team prepared their pipeline incident response plan in close consultation with the Alberta Energy Utilities Board and private pipeline operators, some of whom were developing or revising their own plans at the same time. In 2006, several partners put their plans into action during an exercise staged by a private pipeline operator in Calgary.

"It really tested our interoperability and inter-workings," says Self of the exercise. "There were a lot of lessons learned."

Collective planning like this helps ensure Canadians are back on their feet faster when critical infrastructure is compromised. But the information-sharing goes even deeper.

A pilot project led by the RCMP's critical infrastructure criminal intelligence (CICI) section in Ottawa is providing a conduit for security-related intelligence to flow between government and industry partners in Canada's urban transportation sector.

The suspicious incident reporting system, an electronic tool developed in consultation with transit operators and police of jurisdiction in five Canadian cities, allows authorized transit operators and local police to quickly and consistently log suspicious incidents such as videotaping and bomb threats. The incident reports are then shared with RCMP intelligence analysts and other national security partners, who scrutinize the information to identify criminal trends and potential pre-indicators of terrorist attacks. In the future, a secure web portal will give transit operators and police access to completed, unclassified intelligence reports that could help strengthen front-line security efforts.

This flow of information — from operators to national security analysts and back again — didn't occur regularly before the project began, says Francine Levert, officer in charge of CICI. But it's a crucial link in the chain of public and private sector efforts to bolster infrastructure security and thwart terrorism more broadly.

"If we can detect their (terrorists') pre-operational planning activities, such as intelligence-gathering, reconnaissance and surveillance, it will assist in operational decision-making by law enforcement operators to prevent and mitigate a potential terrorist attack," says Levert.

CICI plans to expand the pilot to other critical infrastructure sectors such as energy and information technology, making it possible for authorized stakeholders to share, analyze and compare security information across sectors. ■

Not your average work suit

Personal protection for CBRNE responders

By Susan Demaray

In order to keep up with the changing threats in the world of chemical, biological, radiological, nuclear and explosive (CBRNE) devices, the RCMP's Explosives Disposal and Technology Sector (EDTS) has to be sure that it is prepared for the unexpected.

"It's a very challenging situation to ensure we have people prepared for this," says Insp John Bureaux, who recently retired as officer in charge of EDTS. "The hazardous materials available to criminals and terrorists are vast. There is a great deal of information on the Internet. We need to keep well informed, trained and equipped (to stay ahead of the threats)."

EDTS receives incident bulletins from bomb data centres around the world, and then uses this information to look for new, emerging threat trends. This leads to the development of new tools and techniques, all with the goal to defuse the threat and to protect first responders, emergency workers and the public. For example, the 1995 sarin gas attack on the Tokyo subway in Japan helped spur the force to develop a program to respond to emerging chemical and biological threats, including moves to incorporate vapour-barrier protective equipment in the existing bomb suit.

A chemical-protection undergarment, made of carbon-impregnated Lycra, was added to protect skin from contact with chemicals and chemical vapours. The outer layer is then added to protect against blasts from explosive devices. The first generation of this integrated bomb suit, providing both blast and chemical protection, was developed in the mid-to-late '90s and is constantly refined as new intelligence is discovered.

"Each year it has been made lighter and there have been dramatic improvements in its protection factors and the flexibility and dexterity factors. You can bend and flex and turn much more easily in this suit," says Bureaux.

The suit is worn by bomb technicians in the RCMP's National CBRNE Response Team, comprised of four regional teams located in Halifax, Ottawa, Edmonton and Vancouver. These teams include members of EDTS, the Forensic Identification Section and partner agencies such as the Department of National Defence (DND) and the Public Health Agency of Canada (PHAC).

Cpl Bruno Solesme, co-ordinator of the Central Region CBRNE Response Team, says that while the suit has it's limitations — it's hot, at about 80 pounds in weight, it's cumbersome, and the helmet restricts one's field of vision — it's an essential tool in personal protection for team members.

"It's going to save my life. It's going to protect me," he says.

Development of the suit and helmet was funded by DND and the RCMP with support from the U.S. government's Technical Support Working Group, and the suit was designed and manufactured in Ottawa by Med-Eng Systems Inc. The suit is now used around the world in more than 90 countries.

"This co-operation with industry has benefited not only the RCMP with a safer, better suit, but many other countries around the world as well," says Bureaux.

The suit is tested using the same type of mannequins used by the auto industry. But instead of car crashes, the mannequins are blasted by bombs and then studied to determine if the suit has met the required protection rating or not.

Once basic testing on the mannequins is complete, the suit is then tested on people in simulated testing situations. The Royal Military College assisted the RCMP in testing the chemical-protective undergarment by using simulated chemical and biological agents to determine how secure the vapour protection was. Then the suit was tested with live chemical agents in the U.K., using a special chamber and detection devices on the skin of a mannequin to determine if any harmful vapour got through the protective undergarment.

Solesme says the CBRNE response teams use the suit during their training exercises, which incorporate scenarios using live chemical and irradiated biological agents. "We deal with the real stuff," he says, so when an emergency situation arises the teams are prepared. "We're trying to imagine what the bad guy would do and to challenge ourselves so we can be ready for whatever we might find." ∎

The CBRNE bomb suit incorporates a vapour-protection barrier undergarment and an outer blast protection shell to protect bomb technicians from the various CBRNE threats they might encounter when responding to a call.

How can police agencies better use technology in responding to disasters?

The panellists

Insp Dennis Erickson, OIC Operational Readiness and Response Co-ordination Centre, RCMP E Division (British Columbia)
S/Sgt Brian Thiessen, program manager, Pacific Region, Canadian Police Research Centre
Derek Prada, general manager, Federal Government Markets Canada, Motorola Canada Limited

Insp Dennis Erickson

Communication and situational awareness are two areas that stand out where increased use of technology could assist police greatly in responding to disasters.

Communication and the ability to communicate quickly and effectively is second in importance only to our employees. As we see time and time again through disasters close to home and around the world, communication systems are often the first things to fail.

As technology develops, the policing community begins to use and ultimately rely heavily upon that technology. Yesterday's pager and phone booth moved to the cellphone, which morphed to Mike phones (cellphones with a portable radio function) and now the BlackBerry. Police radios have expanded to portable repeaters, while portable radios have become stronger and smaller. Technology enables remote police offices, police patrol boats and mobile command posts to access today's modern policing systems via satellite.

Technology also provides us with the ability to utilize more than one communication system thus removing a reliance on one primary system.

Situational awareness is also very important, both in conducting police work and in getting messages out to the public. Getting the information out quickly and consistently to numerous points and locations allows people to make decisions with direct knowledge and confidence from potentially hundreds of kilometres away.

Technology's ability to provide situational awareness not only enhances our knowledge and perspective during an investigation but also assists police and other stakeholders to provide warning, awareness messaging and evacuation alerts for fires, floods and tidal waves, to mention a few.

> **As we see time and time again through disasters close to home and around the world, communication systems are often the first things to fail.**

With today's technology, information updates can be broadcast across television cable or satellite feeds. Emergency radios can be activated by radio signals, which in turn broadcast an emergency message over the radio. This would be akin to your household smoke detector broadcasting an emergency message. Live feeds and public camera systems can be relayed to a police command post or a policy center far away.

With technology systems that are in use or available today, we can make better use of this technology by backing up our systems, providing communication redundancies as opposed to relying on one system and using existing technology to enhance the security for the systems we have in place and the systems we will be moving toward using.

The methods are here and they continue to improve. The challenge for police communities is to fund these opportunities, use other technologies to keep our information safe and secure, then apply the technology to enhance our job and service to the public.

S/Sgt Brian Thiessen

The question makes the risky assumption that police have the needed technology to "better use" in disaster response. The Canadian government's CRTI program is the primary funding agency for disaster/terrorist events. Besides achieving the elusive acronym in an acronym name, Chemical, Biological, Radiological Nuclear, and Explosives (CBRNE) Research and Technology Initiative (CRTI), it has also initiated and funded phenomenal technologies for disaster response: decontamination foam, shielding, portable isolators, rapid detection of hazardous chemicals, medical triage tools, Explosive Ordnance Disposal helmets, and radiation detectors.

Yet, as one member attending his first CRTI summer symposium said, "why haven't I seen any of this in my hands?" Many police detachments have few tools for disaster response. An independent evaluation of CRTI had a similar response, recommending an "engagement model" and "greater exploitation ... to establish an environment for 'technology

pull.'" An article in the summer 2007 edition of Frontline Security recommended a rebate-style program with oversight by the Canadian Police Research Centre or the Public Security Technical Program to resolve the problem. Fortunately, CRTI is working towards overcoming these deployment barriers.

We can better use our technology in disaster response by having it to use.

Having said that, the one technology every police and first responder agency has is radios. Radio communication complaints across police agencies have been frequent after many major disasters: the Vancouver Stanley Cup riots of 1994, the Oklahoma City bombing of 1995, the World Trade Center terrorist attack in 2001, the California fires of 2003, the London bombings of 2005 and Hurricane Katrina in 2005. The same problem can also be seen in day-to-day operations such as police pursuits, crash scenes, search and rescue, and Emergency Response Team operations.

The answer for some is software-defined radios. For others, it is to establish centralized communications such as E-COMM (Emergency Communications for Southwest British Columbia). However, the potential participants in both scenarios are autonomous provinces, cities, municipalities and agencies, each with their own issues, ideas and constraints. Without the corresponding political will of everyone or government mandated participation such as the Police Records Information Management Environment (PRIME) records management system in B.C., not everyone will purchase the radios or join the centralized agency. The problem may be lessened but still remain.

An example is E-COMM, where eight municipalities out of 18 in the Greater Vancouver Regional District (GVRD) have their police, fire and ambulance on the same radio system. This does not include agencies such as public works and search and rescue, which can be critical in disaster response. Nor does it include the other cities and municipalities outside the GVRD, in the Lower Mainland and Fraser Valley of B.C.

We can better use our radio technology in disaster response by being able to communicate with all first responders, interoperably.

Derek Prada

Few would argue that technology is the great force multiplier. It is available to assist first responders in a broad spectrum of their duties. The effective performance of nearly all these duties relies heavily on the officer's ability to communicate verbally and share information with resources either within their own agency or between supporting agencies.

Motorola has been responding to policing and public safety agencies' needs for radio communications during disaster situations for over 65 years. Public safety associations, investigative congressional subcommittees and customers who have dealt with the impact of catastrophic events all agree and testify that interoperable radio communication technologies is non-negotiable, both during and for many months following catastrophic or pandemic events.

Hurricane Katrina accounted for Motorola's single largest recovery response effort in 77 years. Motorola's disaster plan included an extensive field response effort pre-positioning and mobilizing personnel, resources and crews 72 hours prior to the event, working side by side with emergency response personnel to restore affected customer systems within 72+ hours, and rebuilding devastated infrastructure over longer periods.

Despite extensive preparation and planning, Motorola experienced first-hand the strong correlation between time to respond and restore, and degree of planning and preparedness.

Policing and first responder agencies can learn from these experiences through effective preparation and planning, particularly in the following areas:

- First responder/support teams must be able to execute by having a comprehensive human resources plan to consider first responder families in harm's way

- Responders require access to national resources, such as food and shelter, alternative energy sources, and flexible and rapid emergency procurement mechanisms
- They must focus on governance, standard operating procedures, training and exercises
- Effective technology planning requires radio communication system resilience, rapidly deployable mobile radio communication sites, and interoperable radio/voice communication

The reality of the Canadian political environment is that the urgent need for decisive action to fund federal programs for national or cross-border radio interoperability with a national champion driven and supported by Canadian policing agencies simply does not yet exist.

Many independent studies (2003 L'Abbe Report, 2007 IDC Government Insights on Canadian Emergency Management Landscape) have confirmed what most Canadian policing agencies already know: urgent emergency management resource shortages exist due to deficient and erratic funding; federal planning cycles are stagnant, stuck in policy debates between fragmented government stakeholders; and there is a lack of federal funding programs for federal agencies tasked to develop the national vision or agenda, and for national, regional or city policing agencies striving to achieve interoperability projects within their own already stretched budgets.

The result is a lack of national focus, vision and leadership to ensure that policing agencies and first responders will be able to communicate collaboratively when it matters most.

To overcome these obstacles, there is an urgent need for Canadian policing and public safety agencies to pull together with a national policing champion to build their own strong and vocal unified voice. ∎

Facing the challenges of radio interoperability

By Luc Filion
Director, Mobile Communications
Services RCMP

In most cases, police, firefighters and emergency medical services workers are the first to respond at a disaster scene. Their ability to communicate in tense situations where lives may be at risk is crucial. More often than not, the communication tool used in these situations is the police radio.

Emergency preparedness personnel, firefighters, medical personnel and police must be in contact with each other to evacuate the injured and secure the scene. Radio interoperability, which is the ability of a public safety agency to communicate by radio with another public safety agency, on demand and in real-time, can mean the difference between a timely, effective response and disorganized chaos.

Radio interoperability is difficult to attain at the best of times. Different manufacturers make equipment that is incompatible with each other due to various proprietary technologies used by each of their radio architecture, and first responders are usually on different radio systems. Even if two responders are using a radio system from the same manufacturer, different software versions, communication protocols, frequency spectrum usage or vintage equipment will render their systems incompatible. In the end, they often end up exchanging radios so they can talk to each other.

To improve radio interoperability requires a commitment of resources — human and financial — a dose of goodwill among all first responders, and numerous documents and exercises. There are a number of partners in Canada who are participating in efforts to improve interoperability.

The Public Safety Interoperability Directorate (PSID) at Public Safety Canada is spearheading efforts to co-ordinate departments, projects and committees that deal with radio interoperability.

National Defence, Canada Border Services Agency, Canadian Coast Guard, Transport Canada, Industry Canada and the RCMP are participants in this federal working group. PSID is also co-ordinating federal, provincial, territorial and municipal partners.

One of the tools used to guide improvements in radio interoperability is the U.S. Safecom Interoperability Continuum, which has defined a five-pillar radio interoperability framework:

- Governance — a formal governance structure is critical to interoperability planning
- Standard Operating Procedures — formal written guidelines or instructions for incident response
- Technology — although a critical tool for improving interoperability, it is not the sole driver of an optimal solution
- Training and exercises — critical to the implementation and maintenance of an interoperability solution
- Usage — refers to how often interoperable communications technologies are used

The RCMP established its first radio system in 1939. Shared and leased systems — as opposed to RCMP-owned radio systems and manufacturer specific radio system technologies — have made it increasingly difficult to achieve interoperability between radio systems used within the RCMP. Radio system failures due to incompatibilities can endanger police officers and the people they are mandated to protect.

The RCMP is preparing a National Radio Strategy (NRS), which will guide the RCMP and its partners in achieving standard radio system architecture to achieve interoperability, security and sustainability. The NRS will also be made available to partners and will be used as a model by Public Safety Canada for the National Radio Communication Interoperability Strategy.

The engineering of radio systems is difficult at the best of times. Up to 10 years ago, the RCMP owned most of its radio systems. Today, six of the 14 divisional radio systems used by the RCMP are shared or leased systems. This makes it difficult to ensure that all RCMP radio systems are interoperable among themselves, let alone with partner agencies. With the development of incompatible proprietary manufacturer standards, the RCMP has encountered difficulties in ensuring that radio systems are interoperable and sustainable. Sustainable radio systems remain available during disasters because they have redundant equipment and communication paths. Sustainable systems are also engineered and funded to be adaptable, long lasting and possessing a predetermined replacement strategy.

The capability to communicate in a secure manner ensures that proper levels of officer and public safety, confidentiality and interoperability are achieved. Interoperable radio systems ensure that the RCMP can work with its partners when required, whether it is to thwart the efforts of organized crime in Canada or to protect against terrorists in the U.S. Radio systems that are sustainable in emergencies ensure that the RCMP can continue to protect the public they serve.

After the twin tower bombings on September 11, 2001, in New York, radio system interoperability among first responders and emergency management organizations became a requirement in the United States and Canada. Our close ties to the United States demands that our respective police forces and public safety agencies be able to communicate during emergencies, planned events and for joint operations.

Challenges

Obstacles to interoperability abound. One of the challenges is the availability and use of radio frequency spectrum. Spectrum is a limited resource and there are congestion problems in Canada especially within highly populated areas of the country. There is also a need to facilitate the sharing of cross-border spectrum usage through memoranda of understanding or international agreements with the U.S.

The requirements for secure communications and the lack of existing standards have driven the cost of radio systems up over the years. The high cost of public safety-grade radio systems and the difficulty in obtaining funding are major obstacles to renewing current systems with interoperable systems. There are many highly efficient radio systems technologies available; however, they are not compatible with each other and are very expensive. A public safety-grade portable radio worn on the hip of a police officer can cost $6,000 whereas a regular portable radio without the reliability and security of a public safety radio can be purchased for under $1,000. The requirement for system components to be available during times when common infrastructure is down also elevates the cost of system due to the requirement for backup communication links and power supplies.

Finally, there is a lack of co-ordination in systems planning within the public safety community in Canada. Addressing this issue is complex and finding a solution will most likely require all levels of government to co-operate.

Solutions

Fortunately, there are successful radio interoperability strategies and potential solutions on the horizon. Industry Canada, which manages the radio frequency spectrum in Canada, is planning to free up radio spectrum in the 700 MHz Ultra High Frequency for use by public safety agencies. This will alleviate radio frequency spectrum congestion and allow public safety agencies to operate in the same frequencies with compatible

In an emergency, radio interoperability can mean the difference between timely, effective response and disorganized chaos.

Courtesy RCMP Mobile Communications Services

radios to improve interoperability. Within North America, the Association of Public Safety Officials is developing a set of standards known as Project 25 (P25) to ensure that different vendors' radio system components and user gear will work with each other.

Another anticipated but to date unrealized benefit of P25 is the reduction in cost brought about by standard systems. The RCMP has adopted a strategy to procure P25 systems, which are based on common standards and, in most cases, are compatible with existing older radio systems. However, public safety-grade systems will still be expensive compared to other radio systems.

Other groups, such as the Information Technology Committee of the Canadian Association of Chiefs of Police, have entered into a partnership with the Canadian Police Research Centre to create the Canadian Interoperability Technology Interest Group, which will address interoperability issues through projects.

The RCMP has been pursuing efforts to improve interoperability between its own systems as well as with those of its partners.

There are different levels of interoperability. The most basic Level 1 radio interoperability occurs with the exchange of radios at the scene. A gateway or network to link separate radio systems is referred to as Level 2 radio interoperability. At Level 3 radio interoperability, radio equipment conforms to a standard and public safety agencies agree on specified channels. When public safety users agree on an individual radio system, Level 4 radio interoperability is attained, and is only limited by the extent of co-operation between agencies. Common standards-based systems provide Level 5 radio interoperability.

The RCMP uses Level 1 and Level 2 radio interoperability solutions in the majority of its systems and for the majority of its planned or unplanned operations. There are few Level 3 solutions, and even fewer Level 4 solutions. The RCMP's newest radio system in Saskatchewan is the only P25 radio system in its fleet. Once completed in 2008, the system will give the RCMP the opportunity to attain Level 5 radio interoperability with any other partner operating a P25 system in the same frequency band. ∎

The 2003 SARS crisis: prelude to a pandemic?

**By S/Sgt Scott Roberts and
S/Supt Peter Sloly
Toronto Police Service**

On March 5, 2003, an elderly woman who had recently returned to Toronto from a visit to China died from pneumonia-like symptoms. This seemingly innocuous event was the beginning of the very first provincial public health emergency in Toronto's modern history. It was also one of the most unique policing challenges experienced by the Toronto Police Service (TPS).

Several TPS officers responded to the resulting sudden-death call, which is standard operating procedure. Within days of this event, Toronto hospital called the TPS advising that a second family member had died from similar symptoms of sudden onset fever, muscle aches and shortness of breath.

Doctors described the cause of death as atypical pneumonia and worried that it appeared to be highly contagious. On the hospital's suggestion, the first responding officers were tested for this strain of pneumonia. At the same time, a series of media reports began to surface about illnesses and deaths in Southeast Asia attributed to a contagious flu that was being called Severe Acute Respiratory Syndrome (SARS).

The immediate challenges to the TPS entailed attempting to understand the nature and scope of the emerging medical crisis; co-ordinating activities within the service and between relevant external partners; and preparing an appropriate, integrated operational response.

Initial response

Despite these challenges, the TPS immediately began gathering, tracking and analyzing the facts related to SARS from city and provincial medical experts. All potentially exposed officers were identified, contacted and quarantined. The Command co-ordinated various activities both internally and externally. These included producing an information video; purchasing and distributing personal protective equipment; identifying, quarantining and supporting affected members; assisting with security at hospitals; and working with the city and provincial emergency operation centres.

Within 24 hours, the Command produced a video that was distributed to all police members explaining what SARS was, how it was transmitted, what the corporate response was, and how members could protect themselves and their families.

The SARS crisis rapidly escalated at both the local and global levels. On March 26, the Ontario Premier at the time declared a public health emergency. This declaration activated provincial, municipal and health department operations centres. Command members were placed in provincial and municipal operations centres to establish vital information links to other emergency services partners and health sector providers.

The TPS Police Command Centre (PCC) was also fully activated and operational on a 24-hour basis with assigned senior officers rotating on 12-hour shifts as the incident manager. The PCC responsibilities included gathering, recording and disseminating information; identifying and managing health and operational threats; and developing and co-ordinating strategies and tactics.

There were a number of administrative, operational and human resource challenges that the SARS crisis created for the Police Command Centre:

- Quarantine of exposed members
- Health and safety of all members and their families
- Workers compensation benefits for exposed members
- Continuity of police service delivery
- Police security details at hospitals and enforcement of quarantine orders
- Purchase and issue of personal protective equipment
- Prisoner health screening and member decontamination processes
- Increased premium pay and health benefit costs

- An exit strategy to scale down operations
- Additional training from public health and legal services

Voluntary quarantine

Over the course of the SARS crisis, there were a total of 307 TPS members placed into voluntary quarantine. This resulted in just over $560,000 in salary costs, which represented 15,725 lost staff hours of work. Despite this significant loss of human and financial resources, the TPS maintained core services and was able to ensure the safety of its members and the community.

Generally, the TPS responded very well to the SARS public health emergency. The TPS Command quickly grasped the full nature of the unfolding crisis and co-ordinated with health officials to support quarantine orders and provide enhanced security at hospitals. The PCC provided command, control, communication and co-ordination of police operations internally and with external stakeholders.

Members received enhanced information, training, equipment and support throughout the event. The health and welfare of members and their families remained a priority. Despite extensive quarantines, there were no SARS-related deaths nor medical problems among TPS members.

From a community perspective, SARS took a terrible toll on human life,

---

Within 24 hours, the Command produced a video that was distributed to all police members explaining what SARS was, how it was transmitted, what the corporate response was, and how members could protect themselves and their families.

---

increased the level of fear in the community and negatively impacted the financial state of the city due to massive losses of revenue from the tourist industry and increased health care costs.

The TPS operations in response to the SARS crisis did not end with the resolution of the public health dangers. The service became a key partner in re-establishing normalcy in the community, rebuilding the reputation of the city and revitalizing the local economy. It was the Toronto Police Service who planned and organized the massive SARS Rock and Roll Concert that drew over one million fans and tourists to Toronto's Downsview Park to hear notable musicians such as the Rolling Stones.

A TPS after-action report for the SARS crisis identified the following recommendations for improvement:

- Create a pandemic plan within a corporate incident management system (IMS) framework
- Expand IMS and incident command training for senior managers at the service
- Increase IMS training and equipment for front-line members
- Enhance training, equipment and staff for the Emergency Management Unit
- Improve interoperability and co-ordination between police and external partners

Under the leadership of Chief William Blair and with the strategic direction of Deputy Chief Anthony Warr, the TPS has been developing a culture of excellence in emergency management using state-of-the-art-methodologies. The TPS has developed a framework for incident management that focuses on maximizing command, control, co-ordination and co-operation capacity.

The TPS has since completed facility upgrades to enlarge its Public Order and Emergency Management Unit. It has also embarked upon a comprehensive training program for senior officers in emergency management practices and IMS.

What is voluntary quarantine?

During the SARS outbreak, all members of the public —, including police and emergency medical service workers — who were directly or indirectly exposed to the virus, were asked to voluntarily stay home and remain isolated for a period of 10 days.

In total, 307 members of the TPS were placed in voluntary quarantine for 10 days each. They could not leave their homes and had to wear masks — changed twice each day — when in the presence of family members. They could not leave the house (except to an isolated back yard), and could not receive visitors for the 10-day period.

People who were confirmed to have the virus but who refused to comply with a voluntary quarantine, could become the subject of an involuntary quarantine medical order, which police would assist in carrying out.

TPS is finalizing a pandemic procedure and operational plan and has expanded its Chemical, Biological, Radiological and Nuclear program in terms of staff expertise and equipment. The Toronto Police Service is continually testing its operational effectiveness through table-top exercises, full-scale disaster simulations and after-action reports from actual incident management experiences.

SARS was a wake-up call about global and local interdependence. It gave Toronto police a taste of the true tragic potential for the rapid spread of an infectious disease. The police, the province and the city realized that despite tremendous levels of inter-agency co-operation, individual acts of heroism and great examples of leadership, there was insufficient information, infrastructure and interoperability to fully deal with SARS.

The TPS experience through the 2003 SARS outbreak demonstrated the need for police, political, private and public leaders to build greater emergency preparedness capacity and to work in partnership with each other in order to develop disaster-resilient communities. ■

Severe weather forecasting

How police can benefit — and contribute

The technology to predict severe weather has developed steadily over the past 20 years, but advances in software and radar are not the only methods that Environment Canada relies upon to collect information about what to expect. Warning Preparedness Meteorologist Geoff Coulson talks about how new technology together with volunteer networks, including police, can help get the most timely information to those who need it.

By Geoff Coulson
Warning preparedness meterologist
Environment Canada

The last 20 years have seen a number of technological advances that have aided meteorologists in doing things like tracking and forecasting severe thunderstorms and tornadoes. These improvements include Doppler weather radar, a North American lightning detection network, improved weather monitoring software and forecast models and faster, more powerful computers.

However, the human element continues to play an important role in ensuring severe weather watches and warnings reach the Canadian public. The human element comprises the operational meteorologists who work in seven Storm Prediction Centres across Canada and volunteer storm spotters who watch the skies and report occurrences of severe weather directly to the Storm Prediction Centres. This combination of technology and human know-how is the most effective way to ensure Canadians receive timely warnings of approaching severe summer storms.

The technology

Radar
Before the 1980s, conventional weather radar use was the rule in Canada. Conventional weather radar allowed forecasters to track areas of rain and snow and watch how they moved and evolved with time.

However, beginning in the mid-1980s, Canada's conventional weather radars were upgraded to Doppler weather radars, which allowed meteorologists to not only track precipitation, but also get an idea of how the raindrops and snowflakes moved within a cloud. This allowed forecasters to get a sense of how fast the winds were moving at different altitudes above the ground and whether or not there were areas within a cloud showing rotation. Rotation can indicate the possible formation of a tornado.

By the early 2000s, all of Environment Canada's 30 weather radars had been upgraded to provide full Doppler capability. In addition, Environment Canada developed software called the Unified Radar Processor (URP). The URP scans information from a number of radars across Canada and the United States and runs a series of algorithms on this information. This attempts to detect storms that may be capable of producing damaging hail, strong winds, flooding rains and, in some cases, even tornadoes.

The URP ranks individual thunderstorm cells by their potential severity allowing forecasters to quickly pinpoint areas where they should be focusing their efforts. On a busy severe weather day in the summer, forecasters can identify more than 100 separate thunderstorms cells.

> **Reports of damaging storms seen by officers in the field are relayed to local Communications Centres, which in turn pass the information along to the Storm Prediction Centre.**

Satellite imagery

The Storm Prediction Centres use two main types of satellite imagery to track cloud and water vapour patterns in Canada. Geosynchronous or geostationary satellite information comes from a satellite located about 36,000 kilometres above the equator. This satellite rotates at the same speed as the Earth and is therefore capable of providing imagery over the same geographic area every 15 minutes.

Some Storm Prediction Centres such as Edmonton, which produces forecasts for the Canadian Arctic — use polarorbiting satellite information. These satellites orbit at much lower altitudes (approximately 800 kilometres) and provide very detailed information. However, they are only over the same area twice each day. A pair of polar-orbiting satellites can provide imagery over a given area every six hours.

Other networks, software and models
Storm Prediction Centres have access to a
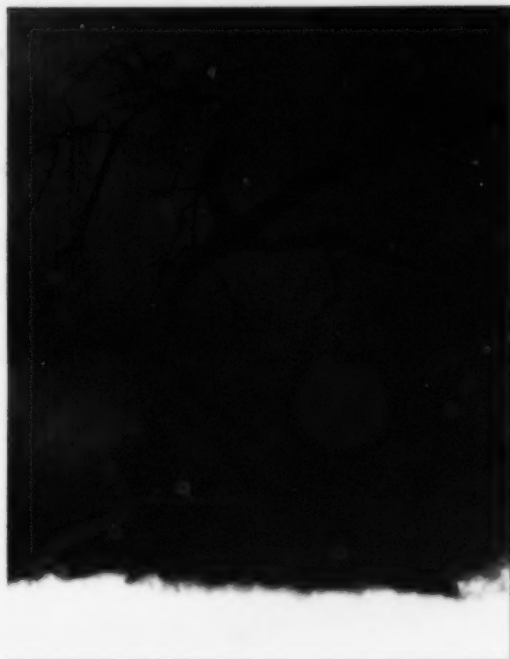
North American lightning detection network capable of tracking lightning strikes to a high degree of accuracy. The strike information is constantly updated to ensure the meteorologists have the most up-to-date information.

A huge increase in computing power in the last number of years combined with ongoing weather research has resulted in a noticeable improvement in the way meteorologists can view, interpret and manipulate weather information. In addition, it has resulted in an improvement in the accuracy of computer models as increased computing power has allowed more realistic future simulations of the state of the atmosphere.

The human element

Meterologists

There is no doubt that developments in technology have aided meteorologists in the last number of years. However, the advances also come with complications. The life of a forecaster used to be somewhat simpler: there was less information to look at and the forecasting process was more straightforward. Today, forecasters have much more information at their disposal. Added to this is the power of the Internet, where additional weather information from a variety of sources is freely available. While more information can be a good thing, it can easily become overwhelming, which is why the teamwork aspect within the Storm Prediction Centre and the sharing of information is so important. No one person can view all of the information on a busy weather day, but a few people working together can get the job done.

Volunteer storm spotters

Summer thunderstorms can develop and move rapidly. Even with the latest in technology, it can be difficult for a meteorologist in a Storm Prediction Centre to know what is actually taking place on the ground. For that reason, Environment Canada has a number of volunteer storm spotters across the country. They know what to look for in the sky or what types of damage that may result from a storm. They quickly report this information to the nearest Storm Prediction Centre.

A number of these volunteers are also ham radio operators and participate in the CANWARN spotter program. Ham radio networks can be set up over an area where damaging storms are expected. A number of volunteers report into a central control person, who then passes the information along to the Storm Prediction Centre.

Police Observing Program

The Ontario Provincial Police (OPP) were added to the list of potential storm spotters in Ontario in 2003. The program with the provincial police was dubbed Project OPPortunity. Reports of damaging storms seen by officers in the field are relayed to local Communications Centres, which in turn pass the information along to the Storm Prediction Centre.

Timely reports of damaging weather can result in warnings being issued or warnings being adjusted to accommodate these real-time reports. This results in better, more complete warnings. Environment Canada is now in discussions with the RCMP to take the successful program in Ontario and spread it to other parts of the country. This initiative is called Project POP (Police Observing Program).

Summer severe weather forecasting presents many challenges. Damaging thunderstorms can develop and move rapidly and seriously impact only a small area. Today's technology allows meteorologists to track these storms better than ever before, but technology alone is not sufficient. Well-trained meteorologists who know how to identify patterns on radar and satellite imagery, combined with real-time reports from volunteers spotters in the field, result in the best solution to this challenging problem. It is this human-machine mix that allows for the most timely and accurate issuance of weather watches and warnings for Canadians. ■

This wreckage was left behind after a tornado moved through Combermere, a small community in Eastern Ontario, on August 2, 2006. Better prediction technology and on-the-ground reports provide essential information when preparing for severe weather.

Courtesy of Geoff Coulson

Does terror terrorize?

Community resilience in Israel

When a community is hit by an act of terrorism, widespread fear and anxiety are almost certain to follow. But consider the community that is regularly terrorized. Are its residents better prepared to cope or rendered dysfunctional by fear? In this article, Professor Alan Kirschenbaum explores this very question based on several research projects he directed in Israel, where terrorism is part of daily life. The results show that humans display a remarkable ability to adapt, and understanding this behaviour could help law enforcement agencies when dealing with terror attacks.

By Alan Kirschenbaum
Technion-Israel Institute of
Technology, Israel

In answer to the question "does terror terrorize?" the mass media's selective presentation of horrific pictures and sounds would lead us to shout out a resounding "yes." Yet, hard research shows a different picture altogether. Not only do people adapt to terror — in its many forms — but they actually develop an increased level of societal resilience that makes future terror events less daunting.

This is not to say that being involved in a terror attack is not frightening and traumatic. It certainly is! But research has shown that such traumatic experiences have little impact on getting back to normal in terms of everyday behaviours in a relatively short period of time. All these findings are a far cry from the image that is promoted by the mass media and in many cases supported by government agencies.

Psychological tactic

In its most fundamental form, terrorism is a psychological tactic that uses violence and particularly the threat of violence to create an atmosphere of fear and anxiety in more people than are directly affected by the acts. Modern terrorism reflects historical forms of terror that were practised by the ancient Greeks and Romans who targeted individuals and became increasingly involved in attacking innocent civilians.

By recognizing today's pervasive nature of terrorist activities globally, policy makers and civilians have begun to re-evaluate terrorism as a major threat to their lifestyles and political well-being. Most persons involved in keeping the peace view terrorism as a threat to the stability of a society with the direct purpose of causing havoc and death to eventually replace one form of government with another.

While terrorist acts occur all over the world, rarely have they been investigated from the point of view of their social impact on groups and communities. Most of what is said in the popular press and television and to some extent in scholarly journals on its societal impact is more opinion than fact.

To rectify this impression, this article will report on a remarkable set of research projects in Israel that looked at the impact of terrorism on both families and communities.

Israel, with a population of about seven million people, is a western-oriented and multicultural society that reflects values and lifestyles found in most western urban societies. This commonality is important because the cultural similarities allow for extrapolation of the results of the research to terror threats in North America and most of Europe.

Background

Terror attacks are nothing new to Israel's population. Even before its independence in 1948, Arab terror attacks against civilians were common. This situation led to the formation of a semi-military organization

This building in Haifa, northern Israel, was hit last year during rocket atta residents developed effective coping behaviours based on social networks.

to provide internal security that has evolved into the present Israel's Homefront Command, similar in objectives to Canada's National Defence Ministry and the United States Department of Homeland Security.

For Israel, the attacks have continued

...attacks fired by Hezbollah. Despite being subjected to daily terror attacks.

for over 60 years. And as anyone listening to the news knows, they continue even today. They have included homicide bombers, roadside bombs, small arms attacks, stabbings, Iraqi ballistic missiles and, since 2001, thousands of Kassam missile attacks. Less than a year ago, over 4,000 Katyusha rockets were fired by Hezbollah from Lebanon, and rained down on over 1.4 million civilians in Israel's north. Given this massive terror campaign, we began asking a fundamental question as to how people managed to survive the almost daily terror attacks.

Adaptation

In a series of research projects from 1999 through 2004, we discovered that there are a large number of ways people reacted to, and as a consequence, changed their behaviours to adapt to terror.

For example, when the Palestinian homicide bombers starting targeting buses and shopping malls, there was a drop in the use of public transportation but an increase in neighbours helping each other out in car pools. Families would only go shopping if there was a guard at the entrance of stores and restaurants.

Informal communications radically increased among family and friends. Both coping and avoidance strategies were used where risk was perceived as greatest. Helping behaviours, religious beliefs and seeking professional advice increased. The net result was that consequences of terror attacks were dissipated through a cushion of social networks, with disruptions to daily life kept at a minimum.

Community resilience

Further analyzing these studies led us to realize that individuals had a diverse repertoire of adaptive behaviours that were socially embedded in their communities, making them more resilient and in fact actually strengthening their resolve.

Supporting these arguments was an in-depth study of communities in and around the Gaza Strip that were daily bombarded by Kassam rockets. Emergent adaptive behaviours actually penetrated deeply into community behaviour by strengthening community bonds. Over time, the social links between individuals, families and their communities increased dramatically in strength. These were self-sustaining social ties that provided a social-based safety net allowing members of the community to not only survive but actually thrive. A combination of intense social networks, ideological and religious beliefs and preparedness explained this remarkable phenomenon.

Intervention

The assumption that terrorism will socially disrupt communities was found in our research to be unfounded. Social networks ameliorate its impact; adaptation behaviours further dilute terror's impact.

Translating these facts into policy protocols leads to the conclusion that it does not make sense to massively intervene in communities where a terror attack occurred. Intervention may interfere with the natural social processes involved and likely contribute to rapid community disruption.

If intervention is chosen, then it should be focused on supporting and strengthening social networks and community resilience rather than creating a "dependent" population that will lose the ability to adapt and cope. This makes social, economic and political sense. It also should remind us that under the surface of communities, there is a large reservoir of resilience that can be tapped.

The adage "Don't confuse me with the facts" is convenient in the mass media but extremely dangerous in terms of how law enforcement agencies should view terrorism, especially how it will affect both policy and operational protocols.

By gaining a greater understanding of the (potential) victim's behaviour and not only that of the perpetrator, police personnel will have a unique tool to develop operational protocols for dealing with terror attacks and helping to prepare communities for future attacks. ■

Alan (Avi) Kirschenbaum is Professor of Organizational Sociology and Disaster Management, Technion-Israel Institute of Technology, Israel. He is past director of research, and consultant to the Population Behaviour Section, Israel's Homeland Command. Professor Kirschenbaum is author of dozens of scientific journal articles and book chapters and recently published the book "Chaos Organization and Disaster Management" (Marcel Dekker 2004).

Are you ready for a large-scale emergency?

By Alain Normand
Manager, Emergency Measures
and Corporate Security
City of Brampton

In my teens, I enjoyed disaster movies. But I later recognized a major flaw in all movies of this type: emergency response is a team effort, not a super-hero scenario.

Police officers are key members of disaster response teams. They are expected to play the traditional roles of traffic control, crowd control and crime scene protection. In situations such as civil disturbances or violent confrontations, police will be asked to take on the more active role in removing the threat.

On occasion, they may also take on some non-traditional roles. For example, in large-scale incidents, police are responsible for access control. Restricting entry into the perimeter to authorized emergency response vehicles is paramount in establishing orderly site control. Police incident command is expected to quickly evaluate the best options for controlling access roads, cordoning off restricted areas and clearing access to emergency vehicles. Police officers may also be instructed to transport essential goods,

During the Northeast Blackout of 2003, one of the main roles for police officers was directing traffic at major intersections. Below, Peel Regional Police officers co-ordinate the assignments and transport of officers to intersections across Brampton, Ontario, a city of over 400,000.

medication or even people.

More diversified roles for police occur during evacuation scenarios. Police officers are by tradition selected to go door-to-door and warn people of a need to evacuate. Volunteers from various social service agencies could take on such a role; however, they will never achieve the level of authority represented by the police uniform. An evacuation order transmitted by a police officer carries much more weight than from a civilian.

At first glance, door-to-door notification may seem simple, but evacuations require more than ringing doorbells. Officers must ensure to the best of their knowledge that occupants have left the property. This may entail having to walk around the yard of a house when nobody answers the front door. It may require reviewing a list with the manager of an office building to ensure all occupants are accounted for. You may even be obligated to enlist the help of a residential building superintendent to conduct an inspection of each apartment.

The most difficult aspect of evacuations comes when people refuse to leave. No legislation exists to remove someone against their will during an evacuation situation. I know of cases where people have wanted to stay to protect their homes right to the last minute, even when confronted with rapidly approaching forest fires.

Some strategies have been used successfully to convince residents to leave their homes. The first is to enlist the help of a family member or a friend. This person can better appeal to the reluctant resident because they may be aware of attachments to other people or better equipped to dismiss reasons for want-

ing to protect the property.

If this fails or the option is unavailable, a friend of mine told me he usually asks the person for next-of-kin information. When the person asks why they want this, he explains how it speeds up the process for communicating the death to relatives. Another officer I know carries a digital camera and a small fingerprinting kit with him and asks if he can take the person's picture and prints. Again, when questioned about this practice, the officer explains how identification of the body is much quicker and paperwork to the coroner's office expedited. These tricks seem to work in most situations because people take a second look at the situation.

A last role in emergency response is securing an area after the evacuation is complete. Unfortunately some people see emergencies as an opportunity to break and enter vacated areas, unhindered by the risk of being spotted.

Getting prepared

As a police officer with the potential to be called to act in an emergency, you need to understand what you may be asked to do and be prepared to take on certain roles for which you are not necessarily trained. So how do you prepare for these new roles?

Being aware of the possibility is your first step to readiness. In other words, know what you may be called to do before the incident occurs. Most municipalities in Canada have an emergency plan and it is a public document. The local plan should identify what primary risks are foreseen in the municipality, how municipal officials intend to cope with emergencies, and what roles will be assigned to police.

Doing your own research can enhance your preparation. For example, if the municipal emergency plan identifies the main risk as a train derailment with a hazardous spill on the line crossing through your town, you may want to take a drive along the rail line. Based on prevailing winds in your area, you can identify potential staging areas that are upwind from the line and at least 1,000 metres away. You can review the traffic flow in the sector and establish the best ways to reroute traffic with minimal interruption.

You can estimate the number of people who may need to be evacuated. Typically about 10 per cent of evacuees have no other place to go. With this in mind, you can calculate how many people you may need to shelter. You should be acquainted with your municipality's shelter plan. You can identify locations of vulnerable populations such as senior homes or schools in the vicinity of the rail line. These populations will become a priority during an emergency.

In small communities, these steps are especially important because you may be the first person on site and take on the role of site manager. This means you will be making the initial assessment of the situation and deciding how to approach the incident. Playing out scenarios ahead of time will give you a definite edge when the emergency occurs.

The second most important element goes back to my initial point about teamwork. As an emergency responder you will be part of a larger response team. The most common challenge in an emergency is communication between the different first responders. I have read reports about how some of the radio systems failed to transmit during the World Trade Center disaster. The consequence was the death of many responders because they did not receive the warning of the imminent collapse of the building. The time to review and test communication systems and protocols is prior to the emergency.

If you are the incident commander, can your communication systems link with the fire and emergency medical services? Does the local fire department use different terminology or protocols to refer to an emergency site? Do you know their incident command structure? Who will you be working with in an emergency? These are all questions to address now.

In summary, readiness means understanding your role, analyzing the risks, familiarizing yourself with the response team, and knowing how to communicate with them.

If you feel you are ill prepared for such situations, there are training and education programs to help you. Colleges and universities are now offering emergency management certificates — some of them online. Networking opportunities also exist through various associations.

The Ontario Association of Emergency Managers (OAEM) is open to people with an interest in the field and is not just limited to experts. It offers workshops and much of the information is on its website. Other provinces are catching on and developing similar associations. If none of this is available, many online courses are available through the Department of Homeland Security in the U.S. Most of the principles that are taught are applicable in Canada.

Someone once said, "Failure to plan is planning to fail." However you wish to approach it, readiness starts now. ∎

Alain Normand directed relief efforts during the Saguenay floods, the Ontario/Quebec ice storm and other emergencies across Canada. He is the current Municipal Emergency Manager for Brampton, Ontario, Past President of the Ontario Association of Emergency Managers, and teaches emergency management part-time at York University and Sheridan College.

Keeping schools SAFE

When an emergency situation happens at a school, like the recent events at Dawson College or Virginia Tech, police need to be ready to respond immediately. The RCMP's new School Action for Emergencies (SAFE) plan puts key information at the fingertips of police responders to schools with the goal of keeping police, students and teachers safe.

"We know that we are going to be responding to these kind of events," says Cpl Anthony Massie, the national SAFE plan co-ordinator. "We're being proactive so that we can be effectively reactive."

Based on the Peel Regional Police School Police Emergency Action Response (SPEAR) program, the SAFE plan puts blueprints, aerial photos, response plans and key contact information in an easily-accessible database so police can have the pertinent information they need at the click of a button. Roadblocks, evacuation routes, entry and observation points are all identified ahead of time and laid out on interactive maps within the SAFE plan database.

"The SAFE plan gives you the ability to see inside the building," says Massie.

Cst Catherine Gillis, in Mission, British Columbia, has been working since the beginning of April to get information for all 22 schools in her district into the database.

She says on average it takes about six hours to gather and input the information for a typical elementary school. That grows to about 10 hours for an average high school. The actual time it takes varies depending on the size of the school and how quickly one gets used to using the SAFE plan database. But she says it's time well spent.

"Unfortunately it's something that's needed now, because of the incidents that are occurring," she says. "It's something you want to make as good as it can be because the information is for other officers. It's about their safety and the safety of others."

The SAFE plan database is easy to navigate, says Gillis, who admits she's not extremely computer savvy. With only a 20-minute phone call with Massie for instruction, she was soon inputting data like a pro. "It looks very intimidating, but it's very user friendly and about as simplified as they can get it," she says.

There are about 300 schools already in the database, with more and more being added with each passing week. The goal, says Massie, is to get every school that falls under RCMP jurisdiction into the program in the upcoming months.

—Susan Demaray

Getting the message right

The dos and don'ts in crisis communication

By Joseph Scanlon
Emergency Communications
Research Unit
Carleton University, Ottawa

When disaster strikes, survivors look to see what needs to be done. Scores — perhaps hundreds — of individuals help others, they dig them out of wreckage and use private vehicles to take the injured to medical centres.

With all these individual acts, it is impossible for anyone to know what is going on. Yet individuals and media call the police: they think you know what's happening.

How should you respond?

- Admit honestly that you don't have immediate answers. A sensible caller will understand you can't possibly know who was on a plane that just crashed or was injured by a tornado that just roared through.
- Ask callers where they are and what they have observed. This will help identify the extent of the impact.
- Tell members of the media how you are responding and when and where information will be available. If there is to be an Emergency Operations Centre, say so, and say where someone will be doing media briefings.

Public warnings

Remember, an effective warning has four criteria. It must be clear about the threat. It must be clear who is being warned. It must be clear about what to do. It must come through all possible sources.

There is a fear that blunt warnings will lead to panic. Not so. Vague warnings lead to confusion. Clear warnings lead to effective behaviour.

When Peel Regional Police evacuated 217,000 people from Mississauga,

Ontario, after a train derailment and chemical spill in November, 1979, they advised the media before starting to evacuate a specific area. They even provided maps. The public expected to have to leave when a police officer came to their door. The warnings were also crystal clear about the threat: the leaking chemicals could lead to more explosions.

Modern technology means some information will spread rapidly no matter what you do. When terrorists attacked London transport, underground survivors sent out messages and visuals long before emergency personnel reached them.

You, too, can go modern. Update your website as information comes in. Use media BlackBerries to send news releases. Update messages on your answering system. In Australia, many who called police about the Indian Ocean tsunami hung up satisfied after hearing a detailed recorded message.

Emergencies lead to widespread news reports, which trigger phone calls from persons who know or think they know someone affected. One way to reduce those calls is to tell the media what areas have not been affected: be as specific as you can.

In an emergency, you won't be responding alone. It is essential to keep in contact with other key responders — fire, Emergency Medical Services (EMS), social services, voluntary agencies — so all speak with consistency.

Finally, it is important to share information with all personnel. Every time a single police officer speaks to someone, that is an act of public communication. Those messages should be consistent. ∎

Joseph Scanlon is Professor Emeritus and Director of the Emergency Communications Research Unit at Carleton University in Ottawa. He has been studying emergency response since 1970.

Planning ahead

Tips for crisis communication

- Use unlisted and unsequenced phones. Otherwise — as has happened to many small police detachments — your phones will be jammed by incoming calls.

- Know how to reach key officials. When phones and radios are overloaded, the best way to contact someone may be to send someone to them.

- Know how to reach media personnel. When a Canadian Pacific Railway Ltd. train spilled chemicals in Minot, North Dakota, at 1:40 a.m. in January, 2002, authorities discovered that all local media operated remotely at night. No radio or TV stations answered calls.

- Know your community. Do some residents need to be reached in a special way? When Point Lepreau, New Brunswick, developed a nuclear emergency plan, its staff realized they might have to contact fishermen in the Bay of Fundy. Since fishermen do not listen to the emergency channel but do talk continually on a chat channel, Point Lepreau decided to use the chat channel in an emergency.

Getting the message right

The dos and don'ts in crisis communication

By Joseph Scanlon
Emergency Communications
Research Unit
Carleton University, Ottawa

When disaster strikes, survivors look to see what needs to be done. Scores — perhaps hundreds — of individuals help others, they dig them out of wreckage and use private vehicles to take the injured to medical centres.

With all these individual acts, it is impossible for anyone to know what is going on. Yet individuals and media call the police: they think you know what's happening.

How should you respond?

- Admit honestly that you don't have immediate answers. A sensible caller will understand you can't possibly know who was on a plane that just crashed or was injured by a tornado that just roared through.
- Ask callers where they are and what they have observed. This will help identify the extent of the impact.
- Tell members of the media how you are responding and when and where information will be available. If there is to be an Emergency Operations Centre, say so, and say where someone will be doing media briefings.

Public warnings

Remember, an effective warning has four criteria. It must be clear about the threat. It must be clear who is being warned. It must be clear about what to do. It must come through all possible sources.

There is a fear that blunt warnings will lead to panic. Not so. Vague warnings lead to confusion. Clear warnings lead to effective behaviour.

When Peel Regional Police evacuated 217,000 people from Mississauga,

Ontario, after a train derailment and chemical spill in November, 1979, they advised the media before starting to evacuate a specific area. They even provided maps. The public expected to have to leave when a police officer came to their door. The warnings were also crystal clear about the threat: the leaking chemicals could lead to more explosions.

Modern technology means some information will spread rapidly no matter what you do. When terrorists attacked London transport, underground survivors sent out messages and visuals long before emergency personnel reached them.

You, too, can go modern. Update your website as information comes in. Use media BlackBerries to send news releases. Update messages on your answering system. In Australia, many who called police about the Indian Ocean tsunami hung up satisfied after hearing a detailed recorded message.

Emergencies lead to widespread news reports, which trigger phone calls from persons who know or think they know someone affected. One way to reduce those calls is to tell the media what areas have not been affected: be as specific as you can.

In an emergency, you won't be responding alone. It is essential to keep in contact with other key responders — fire, Emergency Medical Services (EMS), social services, voluntary agencies — so all speak with consistency.

Finally, it is important to share information with all personnel. Every time a single police officer speaks to someone, that is an act of public communication. Those messages should be consistent. ∎

Joseph Scanlon is Professor Emeritus and Director of the Emergency Communications Research Unit at Carleton University in Ottawa. He has been studying emergency response since 1970.

Planning ahead

Tips for crisis communication

- Use unlisted and unsequenced phones. Otherwise — as has happened to many small police detachments — your phones will be jammed by incoming calls.

- Know how to reach key officials. When phones and radios are overloaded, the best way to contact someone may be to send someone to them.

- Know how to reach media personnel. When a Canadian Pacific Railway Ltd. train spilled chemicals in Minot, North Dakota, at 1:40 a.m. in January, 2002, authorities discovered that all local media operated remotely at night. No radio or TV stations answered calls.

- Know your community. Do some residents need to be reached in a special way? When Point Lepreau, New Brunswick, developed a nuclear emergency plan, its staff realized they might have to contact fishermen in the Bay of Fundy. Since fishermen do not listen to the emergency channel but do talk continually on a chat channel, Point Lepreau decided to use the chat channel in an emergency.

Agroterrorism
A look at the role of law enforcement

The National Institute of Justice is the research, development and evaluation agency of the U.S. Department of Justice. The following research study was conducted through a partnership between the Kansas Bureau of Investigation, the Ford County (Kansas) Sheriff's Department and the National Agriculture Biosecurity Center at Kansas State University. It outlines the challenges facing police in an agroterrorism event.

By the National Institute of Justice
U.S. Department of Justice

Terrorists seeking to strike a blow at the U.S. economy need look no further than the nation's heartland for a "soft" target. An agroterrorist attack could dramatically impact many aspects of American life, including local law enforcement, which — especially in rural areas — is financially and strategically unprepared to respond.

Agricultural experts say that they are most concerned about the intentional introduction of foot-and-mouth disease (FMD) into the food supply. Twenty times more infectious than smallpox, FMD causes painful blisters on the tongues, hooves and teats of cloven-hoofed animals (like cows, pigs, goats and deer), rendering them unable to walk, be milked, eat and drink. Although people generally cannot contract FMD, they can carry the virus in their lungs up to 48 hours and transmit it to animals. The animal-to-animal airborne-transmission range of FMD is 80 kilometres (50 miles).

The introduction of FMD in the United States — with its generally open and difficult-to-protect farms, fields, and feedlots — would require the mass slaughter of animals and the disposal of potentially millions of animal carcasses. It could halt the domestic and international sale of meat and meat products for months or even years. Based on the FMD out-

break in the United Kingdom in 2001, researchers estimate that an attack against the American livestock industry could cost taxpayers up to $60 billion.[1]

Who would lead the response?
Many believe that public health officials would lead the response to an agroterrorism attack, but this might not be the case. The laws of most states require that such an event be handled as a crime scene investigation, giving law enforcement agencies primary responsibility. Ill-equipped to handle the magnitude of responsibilities that would follow an act of agroterrorism, local police departments would be pushed to the limit.

Research points to the first priority of local police after an agroterrorist attack — establishing and enforcing a 10-kilometre (6-mile) radius quarantine around the point of origin to control the spread of the virus. The second priority would be to set up statewide roadblocks to enforce stop-movement orders. Such a tremendous effort — requiring that all vehicles coming into or going out of the impacted state be stopped and inspected — would require a co-ordinated response by local, state and federal officials.

Evidence, including tissue from infected animals, would have to be collected. All cloven-hoofed animals within the affected area would have to be destroyed and disposed of. A full-scale criminal investigation would have to be launched.

Preventing an attack
Because terrorists rely on a lack of preparedness, law enforcement agencies should start now to develop a plan for preventing an agroterrorism attack and preparing for the interruption of basic services, civil and emotional stress, and public health concerns that likely would follow.

On the local level, law enforcement agencies bear a responsibility for intelli-

gence gathering, including the review of federal reports on bioterrorism threats. Local jurisdictions are also in the best position to conduct vulnerability studies of area farms and feedlots.

Specialized training for law enforcement is needed. Joint planning and operational exercises also must take place for agencies to be ready to respond. Partnerships must be created among local farmers, truckers, feedlot owners and other critical members of the food-supply chain. A working relationship between criminal investigators and veterinarians and animal and plant health inspectors must be established.

A new security paradigm
The paradigm for protecting the nation's food supply changed after 9/11, focusing attention on areas that require greater security measures. To protect the nation's 2.1 million farms, the U.S. Department of Agriculture, the U.S. Department of Homeland Security and other intelligence-gathering agencies must work with local and state law enforcement agencies and the livestock industry to develop a national plan to prevent, respond to and ultimately recover from an incident of agroterrorism. ■

1. See Economic Impact of a Foreign Animal Disease Outbreak Across the United States. U.S. Department of Agriculture. Washington, DC. 2004.

Putting out the fires

A challenging year for Victoria Police

By Jessica Davison
State Emergency Response
Coordination Unit
Victoria Police, Australia

The State of Victoria, which lies in the southeast corner of Australia, experienced one of its most significant, long-lasting and widespread bushfire seasons last year.

Initially ignited by massive lightning strikes, the 2006–2007 bushfire season grew into a series of 83 fires that burned across Victoria, resulting in an exhausting 10-week battle that ravaged over 1.48 million hectares of land, destroyed more than 51 homes and resulted in the loss of 1,536 livestock.

The firefighting campaign involved the co-ordinated efforts of Victoria Police; local, state, interstate and international firefighting agencies; and a number of state government agencies who all assisted in the response and recovery phases.

Victoria Police is an organization of over 13,600 employees including police members, public servants and protective security officers. They serve the State of Victoria, which has a combined rural and metropolitan population of over 5 million. There are 339 police stations and other facilities across Victoria, with many rural stations in remote locations operated by one officer. In addition to general policing and traffic management duties, the members of Victoria Police also provide specialist support in a number of areas, including emergency management.

The State Emergency Response Co-ordination Unit (SERCU) provides a central focus for internal and external liaison, planning and co-ordination of policing resources for major police operations and emergency incidents. The office also conducts lectures and assists in conducting multi-agency emergency response training exercises. The officer in charge of SERCU is the State Emergency Response Officer, who is the representative of the State Emergency Response Co-ordinator in emergency management matters such as prevention, response and recovery at local, divisional, state and federal levels.

All-agencies approach

Victoria's emergency management arrangements operate under an all-hazards, all-agencies approach, which allows an active partnership between Commonwealth, state and local levels of government, statutory authorities and voluntary organizations. All agencies are consultative in their approach to emergency planning through the key areas of prevention, preparedness, response and recovery.

The Victorian State Emergency Service, the Metropolitan Fire and Emergency Services Board and the Country Fire Authority are the designated emergency services organizations to fight fires and combat floods, and they act as the incident controllers for such events.

Victoria Police is responsible for the response co-ordination in all emergencies except military aircraft and ship incidents, and, in some cases, civil aircraft accidents.

The bushfires

By December 2006, Victoria had been experiencing severe drought, in some areas for more than 10 years. Water catchments had reached record lows, the landscape was parched and the economic impact on farmers was taking its toll.

In the late spring and early summer of 2006 (September to December), Victoria began experiencing extreme weather patterns, beginning with snow falls on November 15, 2006, followed by scorching temperatures of above 40 degrees Celsius in the northwest of the state just six days later.

On December 1, massive lightning activity in the state ignited the first of a series of 83 fires that burned ferociously for two and a half months. Such was the extent of the fires that more than 15,000 volunteer and professional firefighters from Australia and internationally from Canada, New Zealand and the United States, became involved. The final cost of the fires to the community, the environment, industry and the government is still unknown.

Police role

Throughout the fires, Victoria Police were

The 2006–2007 bushfire season grew into a series of 83 fires that burned across Victoria for 10 weeks. The fires ravaged over 1.48 million hectares of land, destroyed more than 51 homes and resulted in the loss of 1,536 livestock.

The Australian Department of Sustainability and Environment

responsible for organizing and managing Commonwealth resources by setting up and controlling the Municipal Emergency Co-ordination Centres (MECCs), managing communications through the media, establishing Police Operations Centres (POCs), evacuating residents, co-ordinating public warnings in partnership with the ABC (a national radio and television broadcaster), conducting registrations and enquiries of evacuated or displaced persons, providing guidance and leadership to the community, and managing road access in and out of the fires including setting up and staffing traffic management points.

Victoria Police were also responsible for disseminating key safety messages to the community to ensure residents were aware of the risk associated with the fires, and they had the capacity to make appropriate decisions about personal survival and household protection.

As Victoria Police's state-level responders, the State Emergency Response Coordination Unit ensured that liaison officers were in place in all government agency communication centres involved in the response and recovery. The State Emergency Co-ordination Centre was activated to ensure a state-level response co-ordination of resources, proper information flow between agencies and that warnings to the public were managed in the most appropriate and efficient ways.

Challenges faced

In the multi-agency debrief held after the fires on June 1, 2007, a number of challenges and lessons learned were identified including better communicating to the communities what partial and total road closures meant; ensuring proper rest for fatigued firefighters, police and volunteers; and co-ordinating all resource requests through the central point of the MECCs.

As a result of the learnings from the 2006–2007 bushfires, emergency management legislation is under review and improved training will be addressed.

Outcomes

Overall the campaign was successful with zero loss of human life. All agencies

co-operated fully with each other and worked extremely well together.

Victoria's main water catchments were protected through the hard work of our fire agencies, and, as a result, a new Water Replacement Policy was established. The policy states that in the event of fire, regardless of where it starts, if water is taken from domestic and stock or irrigation dams, water needed for essential use will be replaced. This means that a reasonable and sufficient volume of water will be provided to sustain the health of affected residences, pets and livestock.

Another significant impact of the fires was an electricity disruption in January, caused by the fires burning near the major power lines that supply Victoria from interstate. This potentially could have left the state of Victoria without electricity and consequently affected essential services for an indeterminate amount of time. Emergency services, power supply companies and police quickly responded to the outage, which was resolved late into the night with power restored to the affected areas.

Preparations for the 2007–2008 bushfire season are well underway, including a Victoria Police bushfire briefing scheduled for October. Meetings have been held with the Department of Education to ensure that all public and private schools are well-prepared for the future fire seasons.

Partnerships between Victoria Police and our government and emergency services agencies continue to strengthen.

From fire to floods

By June 2007, the environment and the communities affected by the fires were slowly beginning to recover, although the drought continues and the land is still hardened and dusty.

On June 27, the Bureau of Meteorology issued a severe weather warning for flash flooding and widespread damaging winds across the southeast. Soon after, the torrential rains began.

The fire-devastated ground could not cope with the sudden downpour, and water ran off the ground and flowed into the dams and rivers, which in turn broke their banks

Following one of its worst bushfire seasons to date, the state of Victoria endured torrential rains and massive flooding. Police once again activated their Municipal Emergency Co-ordination Centres to co-ordinate the response and recovery.

and flooded into towns, houses and roads.

The flooding threatened to cut off entire communities. Frantic efforts to sandbag houses against the rising flood levels were swiftly overwhelmed. With the roads under water, land access was impossible.

Victoria Police quickly responded and mobilized police helicopters, police boats and personal water crafts while the military supplied additional air support and transport to assist members of the community. People were winched to safety — though many refused to evacuate — and emergency shelters were set up.

Locally, Victoria Police members again activated their MECCs to co-ordinate resources and to centrally gather information to relay up to the state level. All response and recovery government agencies kept in close and constant contact throughout the floods to ensure once again a successful all-agencies approach.

Thankfully again, there was no loss of life, although the economic loss and damage value estimate is expected to be in the tens of millions of dollars.

All agencies worked together in a co-operative and professional manner, and the lessons learned from the floods will soon be discussed at an all-agencies debrief. ■

Just the facts

Doping, betting rings, match-fixing, riots: crimes like these often attract as much attention as the sporting events that sustain them. And it's not just high-level athletes who are affected. Fans, sports organizations, legal systems — even children — take a hit. As we prepare for the Beijing 2008 and Vancouver 2010 Olympic Games, here is a snapshot of sport-related crimes and their impact.

The International Olympic Committee will test 4,500 athletes for drug use during the Beijing 2008 Summer Games. That's a 90 per cent increase from Sydney 2000.

Over 80 per cent of illegal steroids come from black market sources.

A 1998 study by the RCMP on the attitudes of youth towards doping in sport found that one out of five youths aged 12 to 17 used doping substances to improve athletic performance.

In 2005, several employees of the California-based Bay Area Laboratory Cooperative (BALCO) were charged for engaging in schemes to create and distribute undetectable performance-enhancing drugs for athletes, including World Championship medallist sprinters Kelli White and Dwain Chambers.

Most athletes test positive for doping because they fail to stop using a prohibited drug before it is eliminated from their bodies pre-competition.

In November 2005, a German soccer referee received a 29-month jail sentence for fixing the scores of several games, including one German Cup game, in support of an organized betting ring.

The Vietnamese government's "clean hands" campaign against betting and corruption in soccer busted 348 betting rings and seized over $219,000 US during the 2005-2006 Vietnamese soccer season.

More people bet on the Super Bowl than any other sporting event. In Nevada, Americans wagered over $93 million US on the 2007 Super Bowl — almost 40 per cent of the total $2.4 billion wagered on all sporting events in 2006.

A 2006 Arizona Criminal Justice Commission survey found that one quarter of 47,438 grade 8, 10 and 12 students surveyed admitted to betting on team sports at least once in the last month. Over four per cent admitted to placing bets almost every day.

Ticket scalping is big business: one study estimated that ticket brokers and scalpers raked in over $87 million US from live sport and entertainment events in 2000.

One hundred and thirty-seven people were arrested and 21 injured in riots before a tense England-Germany soccer game at the 2000 European Championship. Rampaging fans destroyed cars, broke windows, smashed up bars and clubbed bystanders.

Vancouver Police estimated that a successful 2007 Stanley Cup playoff run by the Vancouver Canucks NHL team could rack up over $2.1 million in extra policing costs to maintain order in downtown streets.

The U.K. Home Office has earmarked £600 million to cover policing during the London 2012 Olympic Games.

SOURCES: Olympic Movement: www.olympic.org; *Royal Canadian Mounted Police:* www.rcmp.gc.ca; *BBC News:* http://news.bbc.co.uk; *The New York Times:* http://www.nytimes.com; *Viet Nam News:* http://vietnamnews.vnagency.com.vn; *American Gaming Association, 2007 Survey of Casino Entertainment:* www.americangaming.org; *Arizona Criminal Justice Commission, 2006 Arizona Youth Survey:* http://azcjc.gov; *The SMART Journal:* www.thesmartjournal.com; *CBC News:* www.cbc.ca

Reducing crime in the North

By Marie Cameron
Yellowknife Detachment, N.W.T

In an effort to reduce crime in downtown Yellowknife, Northwest Territories (N.W.T), RCMP Yellowknife Detachment, alongside its supporting partners, launched an initiative in November 2006 called the Crime Reduction Strategy. Based on models developed in the U.K., New Zealand and British Columbia (B.C.), the Crime Reduction Strategy provides the detachment with the opportunity to work with criminal justice resources and private sector organizations to lower the crime rate.

Crime reduction uses evidence-based techniques, external partners and results-based accountability to drive down the crime rate and reduce the public's fear of crime.

Yellowknife Detachment's Joint Management Team applied the base model of crime reduction to the challenges faced by the detachment. The team began with a basic question: "Who or what are our biggest problems in day-to-day activities?" It identified the most prolific repeat offenders — persons who may have committed nuisance offences that did not result in official charges and were not routinely investigated. The offender would spend the night in detention and when sober would be released without charges, in some cases resulting in 100 repeat offences per year, per individual. The goal was to create a situation in which these repeat offenders could be brought into the justice system and offered resources.

Repeat offenders

Yellowknife Detachment's four watches identified nine individuals who were constantly creating problems by committing nuisance offences and were likely good candidates for rehabilitation. The information packages for the identified repeat offenders listed the number of times police had dealt with them in the last year. The arresting officer(s) could then use the information to arrest the offender with a charge that would stand up to the court process. By charging and convicting the individual, the appropriate resources could then be brought in.

The program's success can be attributed to the participation and co-operation of various criminal justice resources. Together with the Salvation Army, Yellowknife Health and Social Services, Corrections Services N.W.T, Probation Services N.W.T, Justice Canada, N.W.T Department of Justice, Public Prosecution Service of Canada (PPSC), mental health workers and the private sector, RCMP Yellowknife Detachment used a co-ordinated approach to provide the offenders with the resources they needed to address their underlying problems.

The PPSC designated one Crown Counsel to deal with the cases so that there was a consistent approach before the courts. Referring to court case law from the Alberta Court of Appeal, the Crown Counsel argued that although the types of offences committed by the repeat offenders were considered nuisance offences, the Court has recognized the seriousness of the offences and has been prepared to impose a jail sentence. The Territorial Court has been receptive and has imposed the sentences suggested by Crown Counsel.

Measurable results

The success of the initiative has relied, in large part, on the efforts of the members at the Yellowknife Detachment. They have concentrated on putting together a court package that clearly demonstrates a crime had been committed. Their hard work has resulted in noticeable and measurable results, namely a drop in complaint rates received by the detachment. In a monthly comparison, complaint rates fell by 9.57 per cent in January, four per cent in February and 12 per cent in March 2007. Insp Roch Fortin, who spearheaded the project in Yellowknife, estimates the program has resulted in the reduction of hundreds of police man hours.

Since the identification of the initial nine individuals, the program has seen four offenders enter the system. The four who have been sentenced accounted for more than 370 calls for police assistance over the last year. These offenders have been convicted and sentenced for a total of 12 charges. Two more identified offenders are before the courts.

The reactions to the program have also been positive. In some cases, family members and the accused have thanked the authorities involved for intervening and giving them a new chance at life.

The hard work and dedication of the pilot project team in B.C. was the building block for the Yellowknife program. Adjusting B.C.'s initiative to reflect the northern policing environment highlighted the adaptability of the crime reduction strategy. Whether this strategy is used at a two-person detachment or a 200-person detachment, the key is identifying the problem areas and co-ordinating available resources. ■

LECTURE, TICKET OR TOE TAG?

Roadside wildlife requires more than a passing thought

By Roy V. Rea
Ecosystem Science and Management
University of Northern
British Columbia

About 20 years ago, when I was a young impressionable driver, I was pulled over by a California highway patrol officer. I stepped out of my '71 Olds Cutlass and walked to the back of the car to meet the officer, a manner I had been taught by my father.

The officer approached me brandishing a weathered citation booklet. "Ticket or lecture?" he said, as if this were his standard salutation. Time stopped momentarily. "Pardon me?" I replied. "Do you want a ticket or a lecture son?" he reiterated, half annoyed but not

surprised. "Lecture, Sir," I replied, fast enough to make up for having to ask for clarification the first time.

The lecture I received from the highway patrol officer that day was long, but cheaper than a citation. More importantly, however, the lecture opened my eyes to the impressions that a veteran police officer, fully aware of the dangers of unsafe driving, can leave on a young mind. I've never blown a stop sign since.

Although the "lecture or ticket" strategy may be rarely used in highway patrol, lecturing motorists is a technique that in the realm of wildlife-vehicle collision mitigation would, in my academic opinion, have real merit.

As a researcher and educator interested in the interactions of wildlife and

motorists, I've come to realize that school lessons, public announcements, pamphlets and other such outlets have their place in conveying information to the motoring public about the dangers of meeting moose and other game animals on dark Canadian highways, or any highways for that matter. However, information from a police officer armed with data, a citation booklet, anecdotes and photos about what accident scenes with animals look like would likely be more impressive.

Powerful statistics

Having just helped to complete an in-depth analysis of 77,000 accidents between 1996 and 2005 on wildlife-vehicle collision patterns in northern British Columbia, the RCMP in our area now have at their fingertips a set of statistics that outline when and where motorists are most likely to strike animals. Information that can be used by police agencies to predict collision occurrence and teach motorists about collision risk is powerful stuff.

Like officers in northern B.C., highway patrols across the country should request — no, demand — access to wildlife collision statistics for their jurisdictions. Provincial stats are better than no stats, but regional and community-specific statistics on what animals are being hit, at what time of year and time of day, are much better. Collision patterns with deer on Vancouver Island are different than patterns of moose collisions in Prince George and patterns of bison strikes in the Peace River country.

Once armed with the data, officers should obtain some graphic but inoffensive photographic evidence of what a collision with a large animal can do to a minivan. I also recommend officers gather anecdotes from colleagues who have attended accident scenes. Some stories, like pictures,

Between four and eight large animals are struck by vehicles every hour in Canada — that could be over 70,000 killed every year.

Roy V. Rea
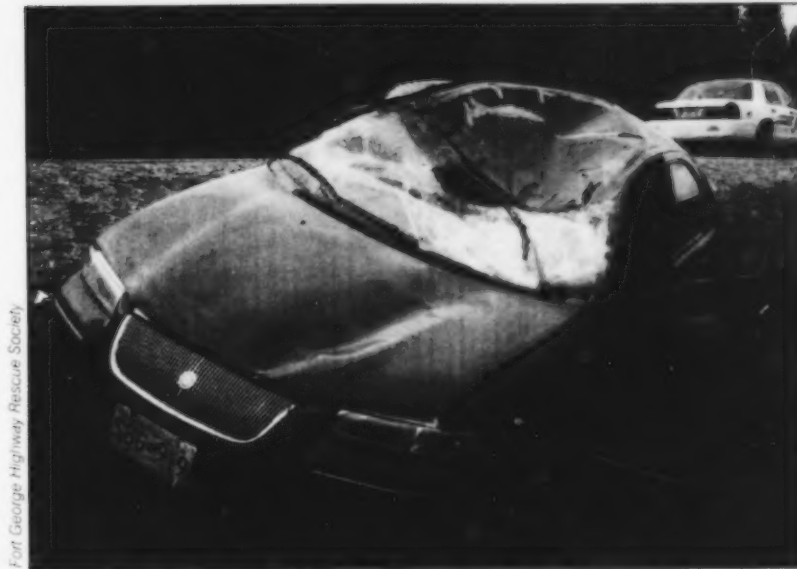
The owners of this car struck a moose north of Prince George, B.C., in 2004. The driver sustained severe neck injuries and three years later is still under medical care. The passenger suffered relatively minor injuries and has made a full recovery.

In short, if lectures or citations can impress drivers enough to facilitate even the slightest change in the way they view the road and the uncertainties that lurk in the dark, the gains may far outweigh the pains. Better to sport a thinner wallet than a toe tag. Who knows, such a lecture-based approach may even help to convert the contempt some drivers feel for "cops" to a sense of gratitude toward an officer of the law who took the time (as one did for me some 20 years ago) to share potentially life-saving information.

Finally, where possible, officers can help build locally relevant databases that can be used to help determine risk by recording four simple pieces of information when attending a wildlife-vehicle collision in their jurisdiction.

The time of day and day of the year when collisions occur are presumably always recorded in accident reporting. However, in addition to these two pieces of information, recording the species of animal involved and the exact location of the collision can eventually allow researchers to determine species-specific patterns of animal movements near roadways for use in road safety planning.

This information, along with recommendations from officers who are in the field and dealing with collisions first hand, provides powerful information that can be used by road safety planners for mitigating collision risk and helping to save the lives of motorists and wildlife. ∎

have a way of leaving indelible etchings in our gray matter.

Next, particularly during peak animal-collision season, officers (if they are not already doing so) should do a quick inspection of vehicles that they pull over and cite drivers for things that could impair their ability to detect an animal and increase their odds of a strike, such as poor windshield clarity, headlight malfunctions and driving without corrective lenses.

Instructing motorists that a cracked windshield not only impairs visibility, but also reduces the integrity of the windshield to withstand an impact from an animal, may decrease the pain associated with getting written up. Convincing motorists to observe recommended nighttime driving speeds (most animals are struck at night) and to generally slow down increases the odds of a driver being able to brake and stop in time for an animal, or any other object for that matter.

Tips for safe driving

Drive during the day

If you can, avoid driving at night. Most collisions with large animals occur at night when animals are most active and difficult for drivers to see.

Slow down

Drivers should buy themselves time to react by resisting the tendency to speed up on straight stretches of road where wildlife collisions occur more than might be expected. If you drive 70 kilometres per hour with standard headlights, you will not have time to stop for anything in your path — a moose or a fallen tree.

Animals are different than people

It sounds elementary, but remembering that difference is critical when driving. Animals may not recognize that a vehicle means danger or that the sound of a horn means watch out. They are often attracted to the road and roadside area for food and do not think of them as dangerous.

Deer whistles don't work

They aren't loud enough to be heard and are at the wrong frequency.

Swerving is very dangerous

In most situations, it is better for motorists to use their brakes instead of their wheel to avoid animals.

—By Gayle Hesse,
Wildlife Collision
Prevention Program

For more information on wildlife collision prevention, visit

www.wildlifecollisions.ca

Related info:
www.gnb.ca/0113/moose/alert-e.asp

The intelligence cycle
Why analyst-client feedback is crucial

By Cst Kelly Ross and Cst Dale Duchesne

The intelligence produced from within a police agency is not unlike intelligence obtained from outside the agency or from tips, source information, Crime Stoppers and other sources. However, when intelligence is produced internally, especially with unsolicited intelligence products, there is often no formal method for tracking and evaluating it. If a law enforcement agency is to remain at the forefront of intelligence-led policing, the analyst-client feedback loop must come full circle.

Analysts who produce strategic or tactical intelligence typically produce a product that is client solicited. In its simplest form, the analyst or intelligence practitioner is tasked with a problem by the client and asked to find answers to the problem through the intelligence process. Some units are strictly intelligence producing while others have blended functions similar to "field intelligence officers" that are involved in both an enforcement and intelligence role.

Unsolicited intelligence is also produced and forwarded to end-user units that incorporate it into strategic portfolios. It can be passed on to units that are primarily investigative in nature where the intelligence can result in a project or investigation.

Intelligence cycle

One adverse condition that grips analysts who produce both unsolicited and client-directed (solicited) intelligence is not knowing what happens to the intelligence. For the most part, there is no method of tracking intelligence that is not client directed, nor a way to ascertain its value or determine if it is being used at all. Despite the fact that feedback is one of the five steps of the intelligence cycle, there is often no formal or informal method of feedback to the analyst to ensure quality control of each intelligence product.

Unsolicited intelligence is extremely important as it relates to the concept of issue search, which is the search for threats that exist or could exist but are not currently known. While intelligence is generally focused on collecting information about known criminal or national security threats, the need to identify new and unknown threats is paramount, particularly in the post-9/11 era.

The criminal intelligence officer/analyst may, in the process of generating unsolicited intelligence, happen upon a new area of concern. If such unsolicited intelligence is processed through the various intelligence uploads and there is no ownership of the product by an end-user, the threat remains the same. Ultimately, the threat identified as a result of the surfaced unsolicited intelligence goes unchallenged, and the intelligence gap remains.

For the analyst, an intelligence package is usually last seen when forwarded to the end-user. After that, very little is known of what happens with it. Unless the analyst assigns a file number to the intelligence package, there is little chance of tracking its effectiveness and value. Even if this happens, a file number really only becomes a mode of tracking the intelligence product if the end-user in turn creates a file number, links the two files, and the producer solicits a response from the end-user. This is a rare occurrence with unsolicited intelligence.

An intelligence unit is only able to qualify and quantify its intelligence production by tracking the end-user's usage of the products. Again, without a feedback mechanism, the intelligence practitioner or analyst has little capacity to measure the value of the products.

Unchecked, there is also the potential for the intelligence going lost, unread or unused. The unit risks falling into the cycle of producing intelligence for intelligence sake and forgetting that the intelligence itself is nothing without further action.

There is also the matter of time-sensitive intelligence, which will have greater value if it is used within a particular time frame. It is important for intelligence analysts to know if the product has at least been used, in whatever capacity, but this is even more critical with time-sensi-

tive material. It is equally important to know what made the product valuable and where improvements could be made — in other words, what worked and what didn't. This feedback can improve the efficiency and effectiveness of the producer's performance.

Providing feedback

To obtain feedback on its intelligence products, intelligence units should consider adding a feedback form to their packages and products. Such a form does not need to be sophisticated. In fact, the simpler it is to use, the better. The simple form consists of five or fewer open-ended questions about the product, which the end-user is asked to complete and return to the originator. The questions gauge how the intelligence will be used, if not used — why not, what its value is, and how it could have been made better.

The format and questions can be designed to fit any intelligence function in need of a feedback mechanism. Completing and returning the feedback form can be done electronically and consumes only minutes of the end-user's time. In cases where intelligence is delivered verbally, the analyst can document the intelligence provided after the verbal briefing and then forward the document

with the analyst-client feedback form to the end-user to complete and return.

The intangible value of this feedback measure is that the intelligence analyst is subject to a response — good or bad — on the product they have created. In addition, this gives the analyst, alongside the end-user, a degree of ownership of the document and part of the end results.

The feedback has further value in that the intelligence practitioner is now privy to the value and quality of their product as others see it. The end result is intelligence that is used and valuable, and intelligence products and practitioners that become increasingly more efficient and effective over time. The importance of a feedback system is championed by David Maister (1993), who found that in every case, implementing a feedback system resulted in analysts improving their abilities.

Intelligence unit managers can also use the feedback to assess the value of their unit's products, to assist in assessing unit productivity, to determine who their primary clients are or who may be a potential client and, at a strategic level, for issue search and to highlight unforeseen criminal/terrorist trends. The feedback may also be helpful to support existing or request additional resources.

For management, a feedback mecha-

nism can facilitate a more accurate account of the value of its intelligence products: "Those who measure and judge the success and usefulness of intelligence are increasingly encouraged to find a direct link between the intelligence product and the resulting investigative successes" (McDowell, 1999).

Feedback is a component of the intelligence process not solely reserved for reviewing strategic results of policing initiatives. It is critical to the healthy function of an intelligence program at all levels. A feedback form is one way of weaving intelligence theory into police practice. In whatever form it takes, a feedback mechanism offers many benefits for the intelligence practitioner, client and managers. ∎

References

Maister, David H (1993). Managing the Professional Service Firm. New York: Free Press Paperbacks, a division of Simon & Schuster Inc.

McDowell, D (1999). 'Quo Vadis Strategic Intelligence? Overview of the implementation and impact of strategic intelligence. In Strategic Intelligence and Analysis Selected Writings (2000). pp 8-18. Pambula: The Intelligence Study Centre

Feedback form

This simple form consists of five questions that the end-user completes and returns to the originator:

1. Please provide your file number for this intelligence brief.

2. Was this intelligence solicited by your unit?

3. What action do you expect your unit to take as a result of this intelligence brief or what is your reason for inaction?

4. What other information could be included that would be of use to your unit? (Photos, sources, more detail.) Please be specific.

5. How could this brief serve you better?
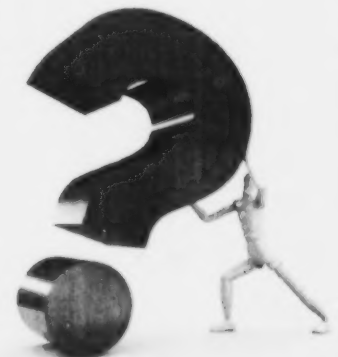
Latest research in law enforcement

The following are excerpts from recent research related to justice and law enforcement. To view the full reports, please visit the website links at the bottom of each summary.

Lessons learned from 9/11: DNA identification in mass fatality incidents

By National Institute of Justice (U.S.)

On September 11, 2001, 2,792 people were killed in terrorist attacks on the World Trade Center (WTC) in New York City. The number of victims, the condition of their remains, and the duration of the recovery effort made the identification of the victims the most difficult ever undertaken by the forensic community in this country (the U.S.).

In response to this need, the National Institute of Justice, the research, development, and evaluation agency of the U.S. Department of Justice, brought together a group of experts to provide advice and support throughout the identification effort. Called the Kinship and Data Analysis Panel (KADAP), the group made recommendations on new forensic technologies, tools, policies, and procedures to help identify those who perished in the WTC attack.

This report contains the KADAP's "lessons learned," particularly regarding DNA protocols, laboratory techniques, and statistical approaches, in the DNA identification of WTC victims. Although New York City's mass disaster plan on 9/11 contained lessons learned from the

1993 terrorist bombing of the WTC, it did not contain policies or procedures for identifying mass disaster victims through DNA analysis. Had this been part of the city's plan in 2001, many of the issues that arose after the attacks could have been more quickly resolved.

This report discusses the incorporation of DNA identification into a mass fatality disaster plan, including how to establish laboratory policies and procedures, including the creation of sample collection documents; assess the magnitude of an identification effort, and identify and acquire resources to respond; identify reference and kinship samples; create a comprehensive laboratory management plan, including technology management and quality assurance; and establish lines of communication between agencies, departments, victims' families and the press.

DNA analysis is the gold standard for identification of human remains from mass disasters. Particularly in the absence of traditional anthropological and other physical characteristics, forensic DNA typing allows for identification of any biological sample and the association of body parts, as long as sufficient DNA can be recovered from the samples. This is true even when the victim's remains are fragmented and the DNA is degraded.

As many of the features described in this report for DNA typing of mass disaster human remains are the same as those for missing persons cases, it may be possible to invest in and co-ordinate with missing persons identification efforts. Thus, the infrastructure for a mass disaster identification process could be in place and only surge capacity would need to be addressed in the event of a mass disaster.

For the full report, please visit:
http://massfatality.dna.gov/

> **DNA analysis is the gold standard for identification of human remains from mass disasters.**

Future directions in technology-enabled crime: 2007-09

By Kim-Kwang Raymond Choo, Russell G. Smith and Rob McCusker

The future of technology-enabled crime sits within the broader digital environment, an environment that is increasingly prone to degradation, infiltration and subsequent criminal activity. Although the precise future characteristics of technology-enabled crime cannot be accurately determined, it remains possible to assess the likely path that future technology-enabled crime risks will take, and which targets are likely to carry greatest risk.

> **It is likely that the incidence of technology-enabled crime will continue to increase over the next two years.**

This report examines the future environment in which Australians will use information and communications technologies (ICT) and how this environment will provide opportunities for illegality and infringement of current regulatory controls. In identifying future risk areas, particular focus is placed on the impact these will have for law enforcement, the need for additional resources, law reform, development of co-operative arrangements between Australian and overseas public and private sector organizations, and development of public information and educational resources to minimize the risk of widespread harm to the community.

Advances in technology bring with them corresponding risks. Some may

be of national importance such as when computer systems that control and operate critical infrastructure are compromised. Other risks have closer impact on the lives of individuals, such as when funds or personal information are stolen. The acquisition and misuse of such information is likely to form the basis of future technology-enabled crime threats.

Computers and computer networks will continue to be both the objects of terrorist attacks and the conduit through which terrorists and other criminals communicate in order to plan and carry out their destructive activities. Because many computer networks transcend international borders, it will increasingly become necessary for all countries to have adequate substantive and procedural laws, and to co-operate successfully to investigate, prevent and to punish terrorist and other criminal activities perpetuated with the aid of computers and computer networks.

The rapid uptake of information communications technologies and its convergence with the Internet poses new challenges in the formulation of policing and preventative strategies. It is also likely that the incidence of technology-enabled crime will continue to increase over the next two years, with the number of large-scale, organized attacks taking prominence.

As reporting of incidents increases among businesses and consumers, the capacity of law enforcement to respond in a timely manner will diminish unless additional resources are made available.

The key to future success in controlling technology-enabled crime is the continued development of partnerships between the various stakeholders including industry, academia, government and law enforcement.

For the full report, please visit:
http://www.aic.gov.au/publications/rpp/78/

Habilitation or harm: Project Greenlight and the potential consequences of correctional programming

By James A. Wilson, PhD

The perceived failure of prison to deter criminal behaviour — as evidenced by high recidivism rates and the substantial costs associated with an increasing number of ex-prisoners who unsuccessfully return to the community — has renewed interest in promising rehabilitative approaches. Nothing has fuelled this renewed interest like the recent discussions on Project Greenlight.

Project Greenlight was a short-term, prison-based re-entry demonstration program. It was jointly operated by the New York State Department of Correctional Services and the New York State Division of Parole and administered by program developers from the Vera Institute of Justice.

Project Greenlight was designed to emphasize specific services that would improve certain interim quality-of-life outcomes and, as a result, would affect subsequent criminal behaviour. The developers believed, for example, that helping parolees find stable housing would reduce criminal behaviour. The program also had a job counsellor to help participants develop their interview skills and connect with potential employers, with the goal of better employment, gained more quickly, for a longer duration.

In the Project Greenlight study, 735 inmates were divided into three groups and followed for at least one year after release. The intervention group of 344 inmates received the Project Greenlight programming. One comparison group (referred to as the UPS group) comprised 113 inmates who were released directly from prisons in upstate New York without any pre-release services. The second comparison group comprised 278 inmates who participated in the transitional services program (TSP) already in existence at the facility.

The evaluation found that the Project Green-light program had no effect on the interim outcomes that it was designed to address — including housing, employment and parole.

Several findings were at odds with program expectations. Most notably, Project Greenlight participants' post-release outcomes were significantly worse than those of the TSP and UPS groups. The evaluation found that the Project Greenlight program had no effect on the interim outcomes that it was designed to address — including housing, employment, and parole — and that Project Greenlight participants fared significantly worse than the two control groups in re-arrest and parole revocation rates at the one-year mark. In addition, although Project Greenlight participants displayed greater knowledge of parole conditions, showed more positive attitudes toward parole, received more service referrals, and reported greater contact with service providers after release, none of these translated into better outcomes.

Project Greenlight had been viewed positively by many people: program developers and staff, participants, corrections officials, policy-makers, and community advocates. It is crucial to recognize that if Project Greenlight had not been evaluated, the program would be regarded as an unqualified success, based solely on the positive perceptions of those involved. Could there be a clearer example of why program evaluations are needed?

For the full report, please visit:
http://www.ojp.usdoj.gov/nij/journals/257/habilitation-or-harm.html

All eyes on airport security

By Karen Sinclair
Halifax International Airport
Authority

The next time you visit Halifax Robert L. Stanfield International Airport, don't be alarmed if you're being watched with greater interest than usual. It's nothing personal.

Just over a year ago, Halifax International Airport Authority (HIAA) launched iWatch, a program designed to increase awareness of security threats and encourage the airport community to report suspicious activity. It's the first and most comprehensive airport security awareness program of its kind in Canada.

Airport security has always been a top-of-mind challenge for Halifax Stanfield International Airport and other Canadian airports, particularly since the events of 9/11. According to the Canadian Air Transport Security Authority (CATSA), over 738,000 prohibited items — including knives, guns and pepper spray — were intercepted at pre-board screening checkpoints in Canada's major airports in 2005. And 2,147 critical incidents, such as the discovery of a prohibited weapon or explosive, occurred at airport checkpoints during the same period.

CATSA reports that its pre-board screening efforts in airport terminals are helping to steadily reduce such incidents. Yet broader airport security efforts pose a different challenge, since terrorist or criminal acts can take place anywhere in the airport vicinity — from the perimeter fence to the parking lot.

"Airports are more than just terminals and runways. They're busy commercial neighbourhoods," says Joyce Carter, HIAA interim president and CEO. "And that means we must be vigilant everywhere there's a possible threat. We believe that a community-focused program like iWatch can help make airport security more far-reaching and effective. When you have security agencies working together with businesses and individuals in the area, you create a powerful network of allies."

This network is vital to helping on-site police and security agencies — including the RCMP, CATSA and Corps of Commissionaire — keep a look-out for suspicious activity. It's this inclusive approach that gives iWatch its distinct community flavour. In fact, HIAA consulted a diverse range of individuals and businesses in the community, from baggage handlers to pilots to ground-service workers, while developing the campaign. One message came through loud and clear: everyone was concerned about airport security and wanted to get involved.

The iWatch program harnesses the commitment of airport workers and provides the tools they need to recognize and report suspicious behaviour. A variety of iWatch posters, brochures and other information continues to be widely distributed throughout the airport community. The material provides clear guidelines on the types of suspicious behaviour to report. Community members are encouraged to "watch out call in" to a central security phone number. Newsletters and updated bulletins also help keep security issues

Courtesy the Halifax International Airport Authority

Danielle, Canjet

Halifax Robert L. Stanfield International Airport is Atlantic Canada's air gateway to the world. Here it is at a glance:

- It is the region's principal full-service airport providing passengers and cargo clients with access to markets across the country, the United States and Europe

- It is the only airport in Atlantic Canada to offer a U.S. Preclearance facility (this allows passengerflying non-stop to the U.S. to clear U.S. Customs and Border Protection prior to their flight)

- It processes 3.4 million passengers annually

- It contributes $1.15 billion to Nova Scotia's economy

- It supports 5,500 employees representing airlines, baggage handlers, retailers, service providers and the Airport Authority

- It is served by 19 airlines offering some 620 weekly flights to 42 domestic and international destinations

- It has nine cargo airlines who ship over 27,500 metric tonnes of cargo annually

- It welcomes 13,000 people to its Air Terminal Building daily

- It sits on 940 hectares of land

- It had Nova Scotia's first escalator installed in 1960

- It is an emergency landing site for NASA's Space Shuttle

Go ahead.
Make eye contact.

Airport security
depends on it.

| Airport Security Action Program | Watch Out – Call In |

iwatch

873-6911

As part of Halifax Stanfield International Airport's ongoing commitment to improve the level of service, its security division works very closely with other agencies within the airport. This includes the Canadian Air Transport Security Authority (CATSA) and involves training both its own staff and CATSA's in responding to individuals who attempt to breach security lines through their areas.

During a recent training exercise, a Halifax airport security staff member donned his civilian clothing and pushed his way through the CATSA pre-board screening security checkpoint, saying loudly, "I am late for my flight." Reacting as they are trained to do, CATSA staff immediately raised the alarm, which alerts the Security Operations Centre and others in the vicinity that someone has breached security.

On this day, unknown to airport security staff, three off-duty Halifax police officers had just gone through their security checks and were on their way to Departures when they heard the alert from CATSA staff and saw our man bolting for the escalator.

They reacted as any police officer would: the three officers tackled him. The "decoy," who is a small person, loudly yelled out at the three burly police officers who grappled him, "it's an exercise, an exercise!"

Everyone involved had a great laugh over it afterwards. The security decoy had a sore neck and declined to be a "runner" again since no one had told him it would be a physical exercise. As for the police officers, a letter of appreciation was sent to the Halifax City Police from the airport security manager thanking them for their timely reaction.

uppermost in people's minds.

"We all have a vested interest in airport security," says Carter. "The ultimate goal of iWatch is to create a security culture that reaches deep into the airport community and helps employees identify suspicious activity that may set off alarm bells, thus reducing security infractions and potential breaches."

The personal safety of the travelling public, airport workers and visitors is a major driver behind the iWatch campaign. Potential terrorist or criminal acts are always on the radar of airport police and security agencies. But airport security incidents, such as unattended baggage or unauthorized people entering secure areas, can also have serious ripple effects. For example, flight delays caused by security breaches can upset travel schedules for passengers and airlines. And these disrup-

tions can cost hundreds of thousands of dollars in lost time and productivity.

Results for the first year of the iWatch program are impressive. Most notably, the program encouraged action. The upshot was a four-fold increase in reports to security from employees throughout the airport community — everyone from cleaners to contractors, retailers to ramp workers.

With a workforce of close to 5,500 people and nearly 11,000 eyes, the Halifax Stanfield International Airport community is better able to keep a closer watch on suspicious activity.

So, airport travellers and visitors shouldn't take it personally if they're being watched with renewed interest. With the help of the iWatch program, workers in the airport community are simply showing their own personal commitment to security. ∎

One way to "tackle" a security breach

As part of Halifax Stanfield International Airport's ongoing commitment to improve the level of service, its security division works very closely with other agencies within the airport. This includes the Canadian Air Transport Security Authority (CATSA) and involves training both its own staff and CATSA's in responding to individuals who attempt to breach security lines through their areas.

During a recent training exercise, a Halifax airport security staff member donned his civilian clothing and pushed his way through the CATSA pre-board screening security checkpoint, saying loudly, "I am late for my flight." Reacting as they are trained to do, CATSA staff immediately raised the alarm, which alerts the Security Operations Centre and others in the vicinity that someone has breached security.

On this day, unknown to airport security staff, three off-duty Halifax police officers had just gone through their security checks and were on their way to Departures when they heard the alert from CATSA staff and saw our man bolting for the escalator.

They reacted as any police officer would: the three officers tackled him. The "decoy," who is a small person, loudly yelled out at the three burly police officers who grappled him, "it's an exercise, an exercise!"

Everyone involved had a great laugh over it afterwards. The security decoy had a sore neck and declined to be a "runner" again since no one had told him it would be a physical exercise. As for the police officers, a letter of appreciation was sent to the Halifax City Police from the airport security manager thanking them for their timely reaction.

uppermost in people's minds.

"We all have a vested interest in airport security," says Carter. "The ultimate goal of iWatch is to create a security culture that reaches deep into the airport community and helps employees identify suspicious activity that may set off alarm bells, thus reducing security infractions and potential breaches."

The personal safety of the travelling public, airport workers and visitors is a major driver behind the iWatch campaign. Potential terrorist or criminal acts are always on the radar of airport police and security agencies. But airport security incidents, such as unattended baggage or unauthorized people entering secure areas, can also have serious ripple effects. For example, flight delays caused by security breaches can upset travel schedules for passengers and airlines. And these disrup-tions can cost hundreds of thousands of dollars in lost time and productivity.

Results for the first year of the iWatch program are impressive. Most notably, the program encouraged action. The upshot was a four-fold increase in reports to security from employees throughout the airport community — everyone from cleaners to contractors, retailers to ramp workers.

With a workforce of close to 5,500 people and nearly 11,000 eyes, the Halifax Stanfield International Airport community is better able to keep a closer watch on suspicious activity.

So, airport travellers and visitors shouldn't take it personally if they're being watched with renewed interest. With the help of the iWatch program, workers in the airport community are simply showing their own personal commitment to security. ■

2010 Olympics
Providing a safe and secure sporting event

By Josué Kibambe Muaka Bambi

Major events and high-profile conferences are becoming increasingly complex in our global high-tech society characterized by increased radicalization, terrorist groups that function like well-structured criminal organizations, and new trends in criminal activities. Terrorism is becoming widely used as a means of getting attention and conveying a message with criminal organizations that exploit every occasion to conduct their activities.

"Securing an international major event such as the Olympics in an era of global terrorism and increased radicalization is a real and complex challenge for national and local law enforcement agencies," says Supt Pierre LeBlanc, director of Major Events at the RCMP. "It requires integrated partnerships at different levels in planning and preparing for all kinds of security scenarios aimed at providing a safe event."

There is nothing new about policing the Olympics. But the complexity and scale of these major events continues to grow, resulting in a greater need for planning and increased policing for host countries.

Since its inception in 2003, the Vancouver 2010 Integrated Security Unit (ISU) has been assigned the challenging task of handling security matters in preparation for the 2010 Vancouver Olympic and Paralympic Games by looking at all potential security issues that could jeopardize the safety of athletes, Vancouverites and visitors from around the world. The RCMP-led ISU, which also includes Vancouver and West Vancouver Police Departments, the Canadian Forces and other security services, is mandated to examine and address an array of complex security-related issues for the Vancouver Games.

Security at the Games

Ensuring the protection of athletes and visitors while not overcrowding the sporting event with uniformed soldiers and police officers is the challenge. While law enforcement agencies will ensure by their presence that order and security prevail during the course of the event, much more will be done to keep the attention on the event itself, which highlights human accomplishment.

The 2010 Vancouver Olympic and Paralympic Games constitute unique challenges for the ISU not only for their international scope, but also due to the unique geographical location of Vancouver as a major international seaport. Criminal groups and terrorists may try to seize the opportunity to enter the country to traffic humans, drugs or counterfeit goods, or to conduct other activities that could jeopardize national security.

Partnership and collaboration

The Vancouver 2010 ISU is preparing for the Games by updating and improving current preventative and defensive measures against terrorists, criminals and anarchist groups who may target either the athletes, the public or officials in attendance. A key component is keeping informed with the latest intelligence on groups or individuals planning on harming attendees at the Games. Combating crime and countering threats to national security during the Games requires law enforcement agencies to work together across organizations and jurisdictions.

The ISU has adopted an integrated approach to ensure the early detection and prevention of potential threats. Integrated planning lets the ISU prepare for various scenarios. With the potential of terrorists targeting critical infrastructure, the ISU emphasizes that interoperability and

B.C. Place Stadium, above, will be one of many sports and celebration venues at the 2010 Olympic Winter Games and Paralympic Winter Games in Vancouver.

Courtesy of VANOC

seamless rapid response remain priorities. Simulations for responding to hostage situations, bomb attacks, bomb threats, terrorist attacks and violent behaviour are but a few of the multiple scenarios planned for by the ISU. Surveillance, intelligence-gathering and preparing for evacuation are other components of security planning.

The integrated approach encompasses more than other law enforcement agencies. The ISU has a close working relationship with the Vancouver Organizing Committee (VANOC), the organization responsible for overall planning for the 2010 Games. For example, a number of venues are being constructed for the Olympics, such as athlete villages. By working with VANOC before blueprints were even designed, the ISU has been able to avoid expensive retrofits for security at a later date.

The ISU is also collaborating with another key unit: the B.C. Government's new Integrated Public Safety Unit (IPSU). Agencies represented by this unit include fire and ambulance as well as health authorities. The ISU and IPSU are co-located to help streamline planning work. Already this new partnership has improved communications among security and public safety forces. The result will be an improved response on a range of potential public safety and security issues, and will be a lasting legacy beyond the Games. ■